
IP8800/S6700, IP8800/S6600, IP8800/S6300, IP8800/S3600,
IP8800/S2400

Troubleshooting Guide

IP88S36-T001-000

Thoroughly read and store this manual.

- Read and thoroughly understand safety-related explanations before using this product.
- Keep this manual in a location close at hand for easy reference.

NEC

■ Applicable products

This manual describes models IP8800/S6700, IP8800/S6600, IP8800/S6300, IP8800/S3600, and IP8800/S2400 series.

■ Caution when exporting

The necessary procedures are to be adopted when exporting this product after first confirming the regulations of the Foreign Exchange and Foreign Trade Law, U.S. export control related regulations, etc.

If any questions remains, please consult with our sales department.

■ Trademarks

Cisco is a registered trademark of U.S. Cisco Systems, Inc. in the U.S. and other countries.

Ethernet is a product name of Xerox Corp. in the U.S.

GSRP is a registered trademark of ALAXALA Networks Corporation.

Internet Explorer is a trademark or registered trademark of Microsoft Corporation in the U.S. and other countries.

IPX is a trademark of Novell, Inc.

Microsoft is a registered trademark of Microsoft Corp. in the U.S. and other countries.

RSA and RSA SecurID are trademarks or registered trademarks of RSA Security Inc. in the U.S. and other countries.

sFlow is a registered trademark of InMon Corp. in the U.S. and other countries.

UNIX is a registered trademark in the U.S. and other countries exclusively licensed by X/Open Company Limited.

VitalQIP and VitalQIP Registration Manager are trademarks of Lucent Technologies.

VLANaccessClient is a trademark of NEC Software.

Windows is a registered trademark of Microsoft Corp. in the U.S. and other countries.

Other company names and product names are trademarks or registered trademarks of their respective companies.

■ Thoroughly read and store this manual

Read and thoroughly understand safety-related explanations before using this product.

Keep this manual in a location close at hand for easy reference.

■ Note

The contents of this manual may be modified at any time for improvement without notice.

Note that output display examples and figures may be different from the actual states.

■ Issue date

November, 2009 (1st Edition) IP88S36-T001-000

■ Copyright

Copyright (c) 2009, NEC Corporation, All rights reserved.

Introduction

■ Applicable product

This manual describes models IP8800/S6700, IP8800/S6600, IP8800/S6300, IP8800/S3600 and IP8800/S2400.

Please read the manual carefully and thoroughly understand the instructions and cautions contained herein before operating the device. Keep the manual in a location close at hand for easy reference when necessary.

Unless otherwise specified, this manual describes functions common to the models. The mark below refers to functions specific to respective models.

[IP8800/S6700]:

The description is applicable to IP8800/S6700.

[IP8800/S6600]:

The description is applicable to IP8800/S6600.

[IP8800/S6300]:

The description is applicable to IP8800/S6300.

[IP8800/S3600]:

The description is applicable to IP8800/S3600.

[IP8800/S2400]:

The description is applicable to IP8800/S2400.

If more than one mark is indicated such as **[IP8800/S3600] [IP8800/S2400]**, the function is only supported by those two models or the description is not applicable to other models.

The mark below refers to functions supported by option licenses.

[OP-NPAR]:

The description is applicable to option license OP-NPAR.

[OP-OPT]:

The description is applicable to option license OP-OTP.

[OP-VAA]:

The description is applicable to option license OP-VAA.

■ Correction of this manual

Contents in this manual may be corrected in the "Release note" or "manual correction document" provided with software.

■ Intended users

This manual has been written for system managers who develop and operate network systems using IP8800/S6700, IP8800/S6600, IP8800/S6300, IP8800/S3600, or IP8800/S2400.

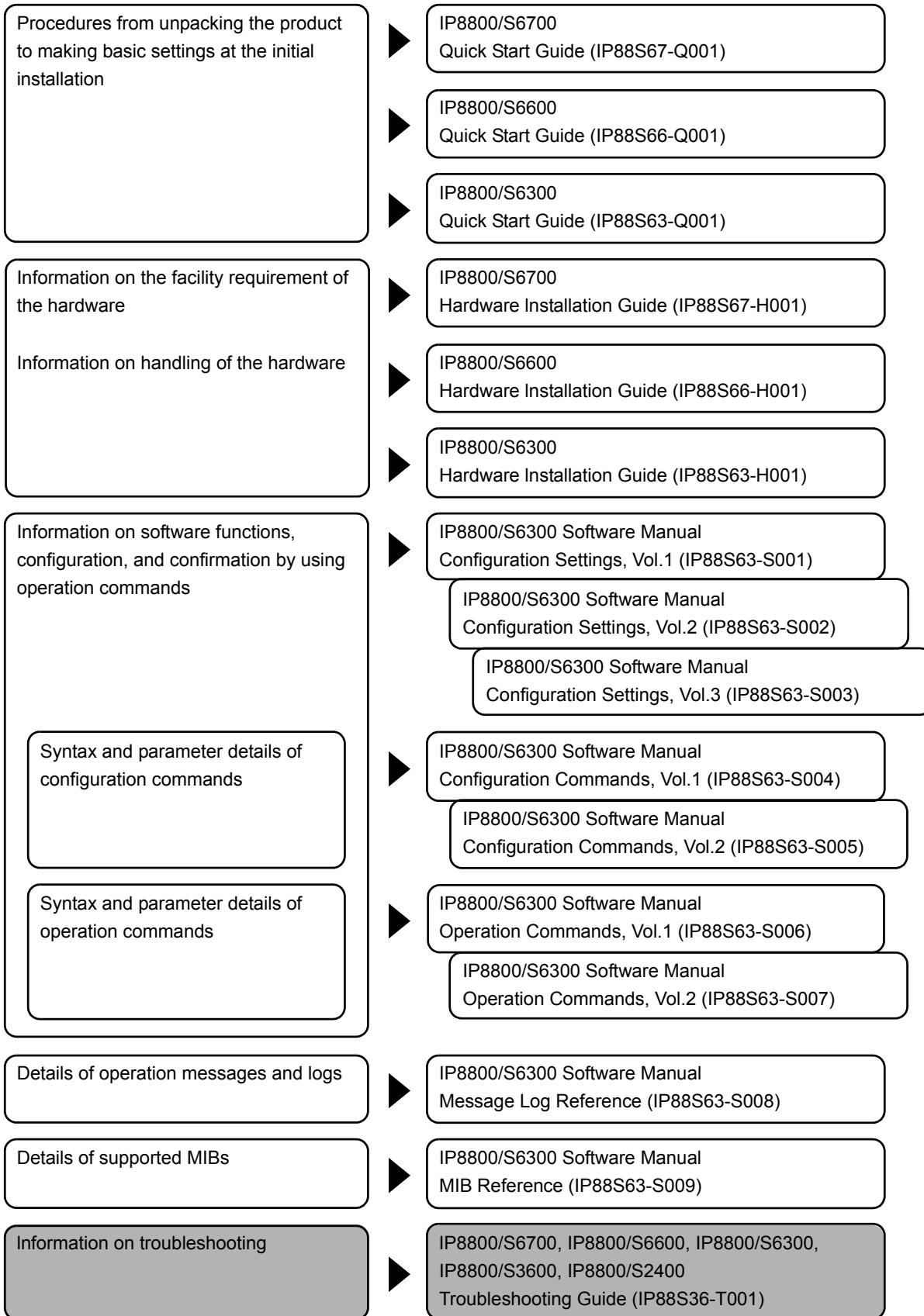
In addition, an understanding of the following is assumed.

- Basic knowledge of network system management

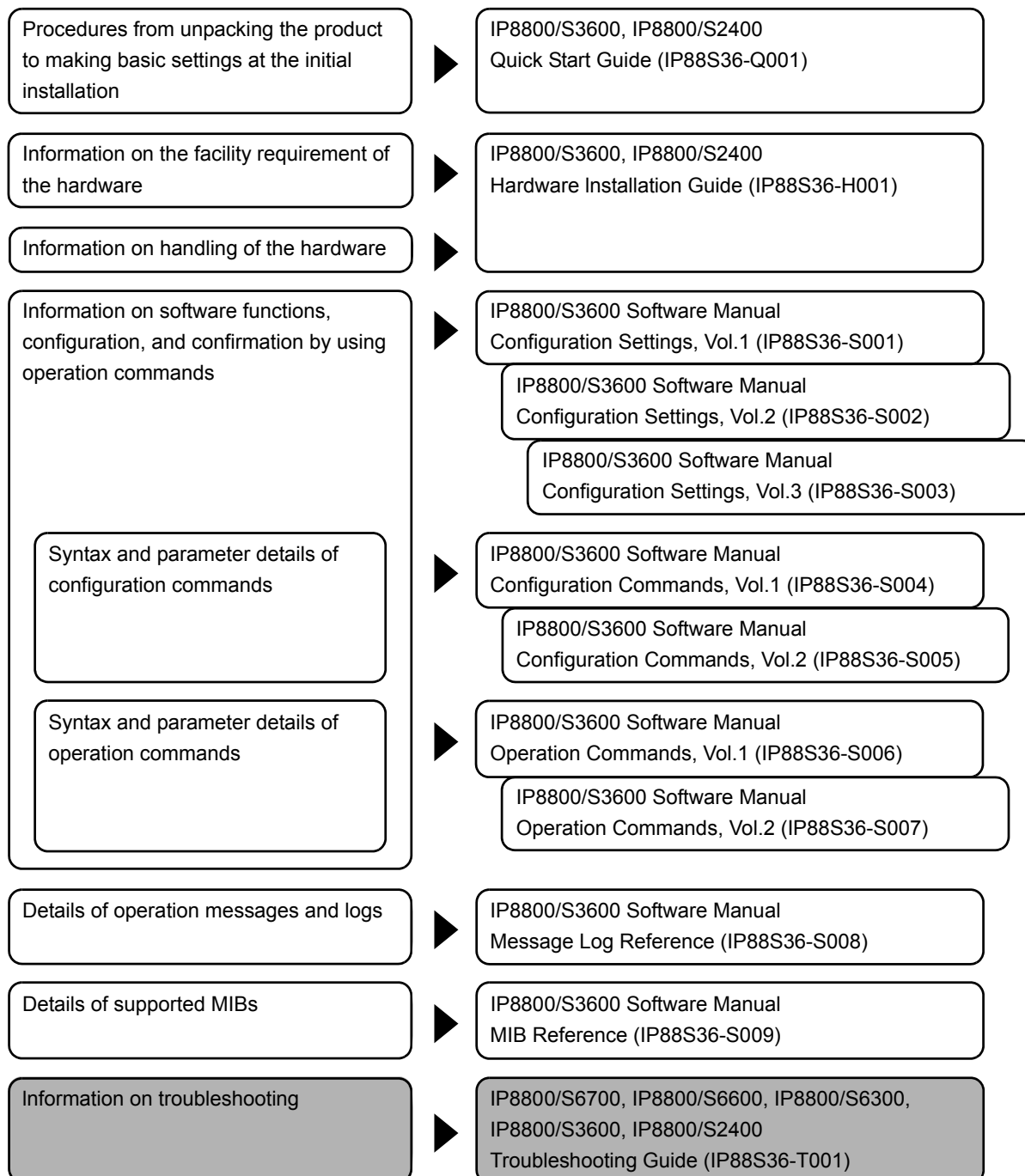
■ Manual referred to

Manuals to be referenced according to the flow of tasks from installation and setup to daily operations are indicated below.

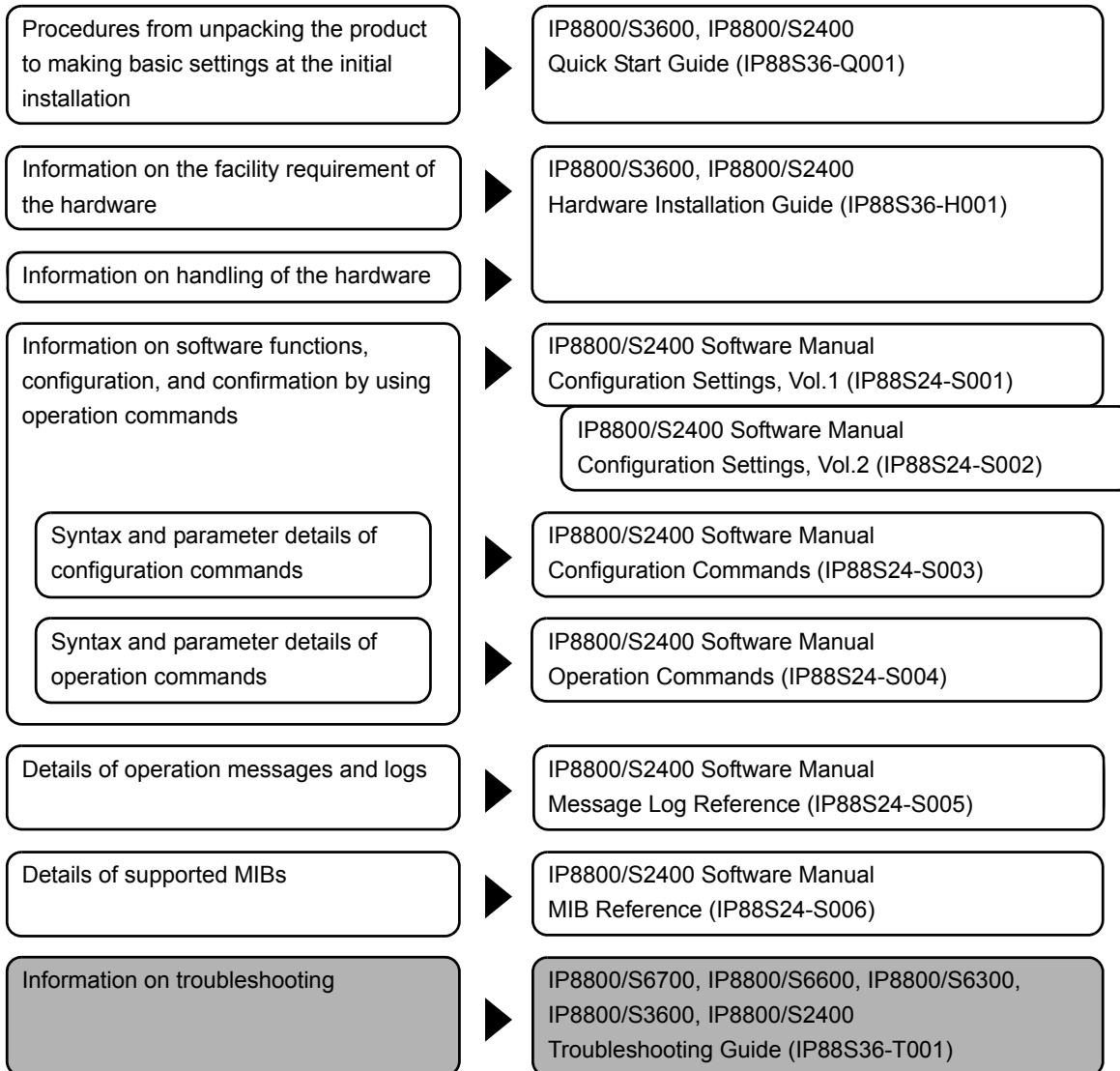
For IP8800/S6700, IP8800/S6600, and IP8800/S6300



For IP8800/S3600



For IP8800/S2400



■ Conventions: abbreviations

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BCU	Basic Control Unit
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second *Usually, abbreviated as bps.
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
BSU	Basic Switching Unit
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing

CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
CSU	Control and Switching Unit
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLPQ	Low Latency Priority Queueing
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LLRLQ	Low Latency Rate Limited Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base

MIP	Maintenance domain Intermediate Point
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MSU	Management and Switching Unit
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NIF	Network Interface
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations, Administration, and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PoE	Power over Ethernet
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
PSP	Packet Switching Processor
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RGQ	Rate Guaranteed Queueing
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SElector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SOP	System Operational Panel
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value

TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
uRPF	unicast Reverse Path Forwarding
VAA	VLAN Access Agent
VLAN	Virtual LAN
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WGQ	Weighted Guaranteed Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

■ Conventions: kB, MB, GB, and TB

1 kB(kilobytes), 1 MB(megabytes), 1 GB(gigabytes), and 1 TB(terabytes) indicate 1024 bytes, 1024^2 bytes, 1024^3 bytes, and 1024^4 bytes respectively.

Contents

Introduction	I
Safety Guide [IP8800/S6700]	v
Safety Guide [IP8800/S6600]	xvii
Safety Guide [IP8800/S6300]	xxix
Safety Guide [IP8800/S3600] [IP8800/S2400]	xli
1 Overview	1
1.1 Failure Analysis Overview	2
1.2 System and Partial Failure Analysis Overview	3
1.2.1 Failure Analysis for IP8800/S6700, IP8800/S6600, and IP8800/S6300	3
1.2.2 Failure Analysis for IP8800/S3600 and IP8800/S2400	4
1.3 Functional Failure Analysis Overview	7
2 Troubleshooting System Failures	11
2.1 Troubleshooting for IP8800/S6700, IP8800/S6600, and IP8800/S6300	12
2.1.1 Troubleshooting Procedure on System Failures	12
2.1.2 Replacement Method of Optional Components	14
2.2 Troubleshooting for IP8800/S3600 and IP8800/S2400	15
2.2.1 Troubleshooting Procedure on System Failures	15
2.2.2 Isolating Failures on External Power Unit	17
2.2.3 Replacement Method of System and Optional Components	18
3 Troubleshooting Functional Failures in Operation	19
3.1 Problems on Login Password	21
3.1.1 Forgot the Login User Password	21
3.1.2 Forgot the System Administrator Password	21
3.2 Problems on MC	22
3.2.1 "MC:-----" is displayed by entering the show system command or the show mc command	22
3.2.2 "MC not found" is displayed when MC is accessed	22
3.3 Problems on Operation Terminal	23
3.3.1 Unable to Input/Display from the Console Correctly	23
3.3.2 Login from the Remote Operation Terminal Is Failed	24
3.3.3 Login Authentication Using RADIUS/TACACS+ Is Disabled	25
3.3.4 Command Authorization Using RADIUS/TACACS+ Is Disabled	25

3.4	Network Interface Communication Failure	27
3.4.1	Ethernet Port Cannot Be Connected	27
3.4.2	Communication Failure in Basic Switching Unit BSU/PSP	29
3.4.3	Actions against Troubles on 10BASE-T/100BASE-TX/1000BASE-T	30
3.4.4	Actions against Troubles on 1000BASE-X	32
3.4.5	Actions against Troubles on 10GBASE-R	33
3.4.6	Communication Failure on Using PoE	35
3.4.7	Communication Failure on Using Link Aggregation	36
3.5	Layer 2 Network Communication Failure	38
3.5.1	Layer 2 Communication by VLAN Is Disabled	38
3.5.2	Failures on Using Spanning Tree	40
3.5.3	Failures on Using Ring Protocol	41
3.5.4	Multicast Relay by IGMP snooping Is Disabled	44
3.5.5	Multicast Relay by MLD snooping Is Disabled	47
3.6	IPv4 Network Communication Failure	50
3.6.1	Communication Is Disabled or Is Disconnected	50
3.6.2	IP Addresses Cannot Be Assigned Using DHCP Function	54
3.6.3	DynamicDNS Cooperation in DHCP Function Is Disabled	58
3.7	IPv4 Unicast Routing Communication Failure	61
3.7.1	No RIP Routing Information Exists	61
3.7.2	No OSPF Routing Information Exists	61
3.7.3	No BGP4 Routing Information Exists	62
3.7.4	No Routing Information Exist [OP-NPAR]	62
3.8	IPv4 Multicast Routing Communication Failure	63
3.8.1	Communication on IPv4 PIM-SM Network Is Disabled	63
3.8.2	Multicast Data Is Double-relayed on IPv4 PIM-SM Network	66
3.8.3	Communication on IPv4 PIM-SSM Network Is Disabled	67
3.8.4	Multicast Data Is Double-relayed on IPv4 PIM-SSM Network	69
3.8.5	IPv4 Multicast Communication Failure In VRF [OP-NPAR]	70
3.9	IPv6 Network Communication Failure	71
3.9.1	Communication Is Disabled or Is Disconnected	71
3.9.2	IPv6 DHCP Troubleshooting	73
3.10	IPv6 Unicast Routing Communication Failure	79
3.10.1	No RIPng Routing Information Exists	79
3.10.2	No OSPFv3 Routing Information Exists	79
3.10.3	No BGP4+ Routing Information Exists	80
3.11	IPv6 Multicast Routing Communication Failure	81
3.11.1	Communication on IPv6 PIM-SM Network Is Disabled	81
3.11.2	Multicast Data Is Double-relayed on IPv6 PIM-SM Network	84
3.11.3	Communication on IPv6 PIM-SSM Network Is Disabled	85
3.11.4	Multicast Data Is Double-relayed on IPv6 PIM-SSM Network	87
3.12	Layer 2 Authentication Communication Failure	89
3.12.1	Communication Failure on Using IEEE 802.1X	89
3.12.2	Communication Failure on Using Web Authentication	92
3.12.3	Communication Failure on Using MAC Authentication	97
3.12.4	Communication Failure on Using Authentication VLAN [OP-VAA]	99

3.13	Communication Failure on High-reliability Function	103
3.13.1	GSRP Communication Failures	103
3.13.2	Communication with VRRP Configuration in IPv4 Network Is Disabled	105
3.13.3	Communication with VRRP Configuration in IPv6 Network Is Disabled	107
3.14	SNMP Communication Failure	110
3.14.1	MIBs Cannot Be Obtained from SNMP Manager	110
3.14.2	Traps Cannot Be Received by SNMP Manager	110
3.15	Troubleshooting of sFlow Statistics (Flow Statistics) Function	112
3.15.1	sFlow Packets Do Not Reach Collector	112
3.15.2	Flow Sample Does Not Reach Collector	115
3.15.3	Counter Sample Does Not Reach Collector	115
3.16	Communication Failures on Neighboring System Managing Function	116
3.16.1	Unable to Obtain Neighboring System Information via LLDP Function	116
3.16.2	Unable to Obtain Neighboring System Information via OADP Function	116
3.17	NTP Communication Failure	118
3.17.1	Time Synchronization by NTP Is Disabled	118
3.18	Communication Failure on IEEE802.3ah/UDLD Function	119
3.18.1	Port Becomes Inactive Due to IEEE802.3ah/UDLD Function	119
3.19	Problems on Redundant Configuration of Basic Control Unit (BCU)/Control and Switching Unit (CSU)/ Management and Switching Unit (MSU) [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]	120
3.19.1	Active System Switchover Is Disabled	120
3.20	Problems on Redundant Configuration of Basic Switching Unit (BSU) [IP8800/S6700]	121
3.20.1	Active BSU Switchover Is Disabled	121
3.21	Problems on Power Saving Feature	123
3.21.1	Schedule Is Disabled [IP8800/S6700] [IP8800/S6600]	123
3.22	Congestion Caused by Packets Processed Through CPU Is Not Recovered	124
3.23	Communication Failure Caused by Settings of Filtering/QoS	126
3.23.1	Checking Filtering/QoS Setting Information	126

4

	Troubleshooting Communication Failures Due to Resource Shortage [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]	129
--	---	------------

4.1	MAC Address Table Resource Shortage	130
4.1.1	Checking Resource Usage of MAC Address Table	130
4.1.2	Action to Be Taken When MAC Address Table Resource Shortage Occurs	130
4.2	When Resource Shortage of VLAN Identification Table Occurs	133
4.2.1	Checking VLAN Identification Table Resource Usage	133
4.2.2	Action to Be Taken When VLAN Identification Table Resource Shortage Occurs	133
4.3	When Resource Shortage Occurs in Shared Memory	135
4.3.1	Checking Resource Usage of Shared Memory	135
4.3.2	Action to Be Taken When Resource Shortage of Shared Memory Occurs	135

5

	Collecting Failure Information	137
5.1	Collecting Failure Information	138
5.1.1	Collecting Failure Information Using ftp Command from the Operation Terminal	138

5.1.2	Collecting Failure Information Using dump Command [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]	140
5.2	Transferring Files for Maintenance Information	144
5.2.1	Transferring Files Using ftp Command	145
5.2.2	Transferring Files Using zmodem Command [IP8800/S3600] [IP8800/S2400]	148
5.2.3	Transferring Maintenance Information Files Using show tech-support Command	148
5.2.4	Transferring Files Using ftp Command from the Operation Terminal	150
5.3	Writing to MC	152
5.3.1	Writing File to MC Using Operation Terminal	152

6	Line Test	153
6.1	Testing Line	154
6.1.1	Ethernet Port	154

7	Restarting the System	159
7.1	Restarting the System	160
7.1.1	Restarting the System	160

Appendix		165
Appendix A	Contents of show tech-support Command Display	166
Appendix A.1	Contents of show tech-support Command Display	166

Index		187
-------	--	-----



Safety Guide [IP8800/S6700]

■ Safety guide for the IP8800/S6700 series

- This document provides safety-related notices for use of the IP8800/S6700 series. To utilize the functions of this device, read this document completely and carefully before using the device.
- Keep this document at hand after you read it, so that you can always refer it later.
- For any operation, follow the directions and procedures given by this document.
- Observe the cautions labeled on the device or those presented by this document. If you fail to do so, you will cause damage to yourself or the device.

■ Symbols

- We have various symbols displayed on the IP8800/S6700 series and in the manuals to guide you in using the IP8800/S6700 series correctly and safely without injuring yourself and others, or damaging equipment assets. Below are the symbols and their meanings. Fully understand the description and then proceed with reading the main part of the manual.

 WARNING	If you ignore instructions preceded by this symbol, you could cause personal injury or death to yourself and others.
 CAUTION	If you ignore instructions preceded by this symbol, you could cause personal injury to yourself and others, or serious damage to the device or surroundings.
CAUTION	If you ignore instructions preceded by this symbol, you could cause physical damage to the device or surroundings.
NOTE	A note is informational in nature. Unlike warning and caution notices, notes (for prevention of malfunction, prevention of product minor damages) are not related to the physical injury or damage to the device.

■ Operations and actions

- Do not attempt to perform any operations not specifically described in this document.
In case of a problem on the device, contact the maintenance personnel after performing the following.
- For the device with AC power supply mounted, power off the device and unplug the power cable from the outlet.
- For the device with DC power supply mounted, power off the device and turn off the breaker in the power supply equipment.

■ Be careful in operation

- The instructions shown on the device or in this manual are the results of our thorough consideration. However, an unexpected situation may occur. For operations, not only follow the instructions but also always be careful with your judgment.

 **WARNING**

- **In case a failure should occur, power off the device immediately.**
 - In case fume or unusual odor should occur, or foreign matters should come into the device, power off the device as follows. If the device is used in a faulty state, fire disasters or electric shock may be caused.
 - For the device with AC power supply mounted, power off the device and unplug the power cable from the outlet.
 - For the device with DC power supply mounted, power off the device and turn off the breaker in the power supply equipment because the power cable is connected via a terminal.

- **Do not place the device in an unstable location.**
 - If the device is being placed on a table, be sure to install it horizontally on a workbench or the like that can sufficiently bear the weight of the device. If the device is placed on an unstable location such on a shaky table or slope, the device may fall and drop and consequently personal injury may occur.

- **Do not remove the device cover.**
 - Do not remove the device cover. Electric shock may be caused.

- **Do not put foreign matters in the device.**
 - Do not insert or drop metals or combustibles into the device through the intake/exhaust port. Fire disasters or electric shock may be caused.

- **Modification is not permissible.**
 - Device modification is not permissible. Fire disasters or electric shock may be caused.

- **Do not give a shock.**
 - In case the device is dropped or parts are damaged, power off the device, pull the cable out of the outlet, and call the maintenance engineer. Otherwise it can cause a fire or electric shock.

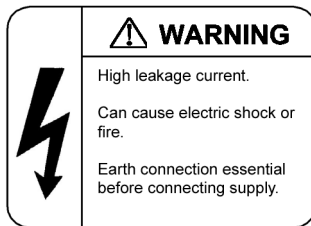
- **Do not put any material on the device.**
 - Do not put a metal such as pin or clip or a container with water in it such as vase or flower pot on the device. Fire disasters or electric shock may be caused.

- **Do not use power not specified.**
 - Do not use a supply voltage not specified. Fire disasters or electric shock may be caused.

- **The current capacity supplied to the power distribution panel must be larger than the operating current of the breaker.**
 - The current capacity supplied to the power distribution panel must be larger than the operating current of the breaker. Otherwise, the breaker may not work in the event of a failure and cause fire disasters.

■ **Grounding is required.**

- When the device is connected to the power supply of 100VAC, leak current of up to 3.5mA flows for each device. Be sure to use the grounded outlet. If the power supply is used without grounding, an electric shock may be caused and failures may occur due to electric noise.
- When the device is connected to the power supply of 200VAC, leak current of up to 5mA flows for each device. Choose a grounded outlet and make sure that the outlet is grounded to a ground plate in the building. Request the maintenance personnel or specialized installation workers to check the grounding. If the power supply is used without grounding, an electric shock may be caused and failures may occur due to electric noise. The label below is attached to the device.



- When the device is connected to the DC power supply, be sure to connect the grounding terminal. If the power supply is used without grounding, an electric shock may be caused and failures may occur due to electric noise.

■ **Installing/uninstalling of the DC power cable must be performed by the trained engineer or maintenance personnel.**

- Installing/uninstalling of the DC power cable must be performed by the trained engineer or maintenance personnel. DC power cable is connected to the power supply via a terminal. Therefore, inadvertent handling of the DC power cable may result in fire disasters or electric shock.

■ **Before installing or removing a DC power cable, turn off the breaker on power supply facilities.**

- Before installing or removing a DC power cable, turn off the breaker on power supply facilities. Operation with the breaker on may cause electric shock.

■ **Attach insulation covers on the 0V and -48V terminals of a DC power cable.**

- Attach insulation covers on the 0V and -48V terminals of a DC power cable (the side of which connects to power supply facilities). Operation without insulation covers may cause electric shock.

■ **When using the DC power supply, do not leave the terminal board uncovered.**

- When using the DC power supply, be sure to attach the cover to the terminal board after connecting the power cable. Operating it without the terminal board cover can cause an electric shock.

■ **Do not touch the potential tap.**

- The power supply is provided with the potential tap. This tap is used for inspection at shipment. Customer should not use this tap. Do not insert a sharp material such as pin or clip into the potential tap. Fire disasters or electric shock may be caused.

■ The device must be carried and installed by the trained personnel or specialized carrier.

- The weight of the device is 82 kg/182 lb at the maximum. The device must be carried and installed by the trained personnel or specialized carrier. Otherwise, a personal injury due to drop or fall may be caused. For installation and carrying of the device, use a handling equipment such as a hand lifter. Otherwise, a personal injury due to drop or fall may be caused. The label below is attached to the device.



■ Handle the power cable with caution.

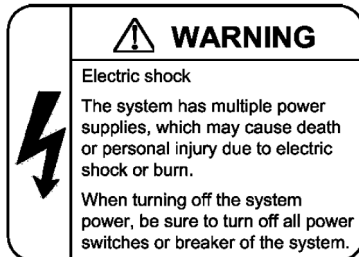
- Do not put a heavy material on the power cable or do not pull, bend, or modify the power cable. The power cable will be damaged and fire disasters or electric shock may be caused. A heavy material may be placed as a result of covering the cable with a floor carpet.
- Use the attached power cable or the power cable complying with the specifications. If any other cable is used, fire disasters or electric shock may be caused. Do not use the attached power cable for other purposes. In such a case, fire disasters or electric shock may be caused.
- If the power cable is degraded (e.g., wire cores exposed or broken), ask the service personnel for replacement. Otherwise it can cause a fire or electric shock.
- Check to see if dust is deposited on the power plug. Insert the plug securely to the end so that shakiness will not occur. If dust is deposited or connection is incomplete, fire disasters or electric shock may be caused.

■ Do not plug too many leads into a single outlet.

- Do not plug too many power plugs into a single outlet. Many loads on an electrical outlet may result in fire disasters and the electric energy in use may be exceeded, the breaker may go off, and other components may be affected.

■ Before powering off, turn off all power switches or breakers on the device.

- Multiple input power supplies are provided to the device. Before powering off, turn off all power switches (when AC power supply is mounted) or breakers (when DC power supply is mounted) on the device. The label below is attached to the device.



■ Work to add or replace equipment must be performed by a trained engineer or maintenance personnel.

- To add or replace optional components must be performed by a trained engineer or maintenance personnel. To add or replace a power supply involves to plug and unplug power cables; a person other than the preceding ones may fail to handle things, which can cause fire disaster, electric shock, and equipment failure. Other optional components, if handled mistakenly, can also cause fire disaster, wounds, and equipment failure.

■ Do not press the switch on the basic control unit with a fragile tip, pin, or clip that may get stuck and cannot be removed.

- Do not press the switch on the front panel of the basic control unit with a fragile tip, pin, or clip that may get stuck and cannot be removed. Fire disasters or electric shock may be caused.

■ Before addition or replacement of the power supply, unplug the power cable.

- Remove the power cable from the power supply when adding or replacing it. With the power cable connected, the power supply equipment may remain energized from some circuits even the power switch is turned off. Therefore, adding or replacing the power supply with the power cable connected may cause a fire or electric shock.

■ Keep air dusters away from fire.

- If you use an air duster with combustible gas to clean the optical connector, keep away from fire. Otherwise, fire disaster may occur.

 **CAUTION**

- **Do not install the device in a humid or dusty environment.**
 - Do not install the device in a humid or dusty environment. Fire disasters or electric shock may be caused.
 - Moving the device from a cold place to a warm place may form condensation on the surface or internal of the device. If the device is operated immediately a fire or electric shock can be caused. Thus, in this case, leave the device as it is for several hours before starting operation.

- **Do not stack the devices.**
 - Do not stack the devices. The device may be damaged. The device may be damaged or lose its balance and fall or drop. As a result, personal injury may occur.

- **Do not recline on the device, or place a heavy loading on it.**
 - Do not ride on or cling to the device or do not put a heavy material on it. The device may be damaged. The device may be damaged or lose its balance and fall or drop. As a result, personal injury may occur.

- **When installing the device on the rack, use the guide rail or shelf.**
 - The rack mounting bracket supplied with this device is used to fasten the device on the rack but not to support the weight of the device. Be sure to use the guide rail or shelf. The guide rail or shelf must be the one attached to the rack and capable of supporting the weight of the fully mounted switch.

- **Do not block the intake and/or exhaust port.**
 - Do not block the intake/exhaust port of the device. Blocking the intake/exhaust port keeps heat inside and fire disasters may be caused. Keep a space of at least 70mm from the intake/exhaust port.

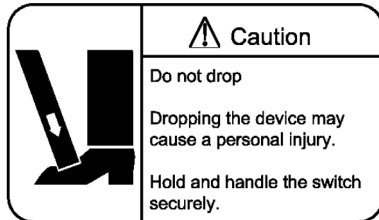
- **Do not bring hairs or any foreign matters close to the intake/exhaust port of the device.**
 - The cooling fan unit is provided on the device. Do not put any material close to the intake/exhaust port. The internal temperature rise may result in a failure. Do not put hair or any material close to the intake/exhaust port. You may be caught and injured.

- **When moving an optional component, do not carry it by holding its handle.**
 - When moving a fan unit or power supply, do not hold its handle. The handle may come off and the device may drop. As a result, a personal injury may occur. Or the fan unit or power supply may be deformed that may cause a fire or electric shock.

- **Before carrying the device, remove the cables.**
 - When moving the device, power off the device, remove all the cables from the device, and then move the device. Otherwise the device or cable may be deformed or damaged. As a result, fire disasters or electric shock may be caused.

■ Do not drop an optional component.

- Handle the optional component carefully not to drop it. If dropped, personal injury may be caused.
- The weight and depth of the DC power supply are 5.6 kg/12.4 lb and 163 mm/6.4 in respectively. When removing the DC power supply, hold it securely. If pulling it forward carelessly, it may drop and cause a personal injury. The label below is attached to the DC power supply.



■ Do not touch the inside of the device.

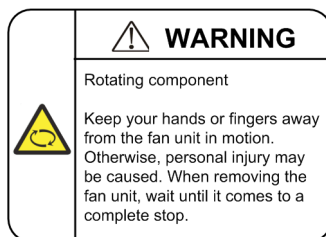
- Do not put your hand inadvertently inside the device. Mechanical parts may cause a personal injury.

■ The basic control unit and network interface component may be hot. Be careful when removing them.

- Parts mounted on the basic control unit and network interface component may be hot: Do not touch them to prevent getting burned.

■ When removing the fan unit, do not put your hand close to the rotating fan.

- The fan may still be rotating immediately after the removal of the fan unit. While the fan is rotating, do not put your hand or finger close to it. Personal injury may be caused. The label below is attached to the fan unit.



■ Do not roughly handle the power cable.

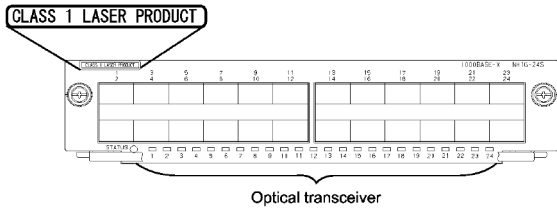
- Do not put the power cable close to the heating apparatus. The cable sheath may be melted and fire disasters or electric shock may be caused.
- When inserting the power cable into the outlet or removing from it, be sure to hold the cable plug. Pulling up the cable with the cable grasped, the wire can be broken.

■ Do not touch the device directly if you have metal allergies.

- This device is coated with metals including zinc, nickel, and gold. If you have allergies to them, do not touch the device directly to prevent getting dermatitis.

■ Be careful of laser beams.

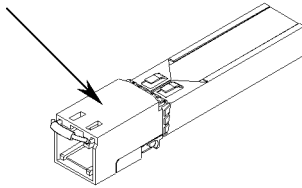
- The network interface module as indicated below uses laser beams. Do not peep in the optical transceiver directly.



■ Do not touch a working (including immediately after stopping) SFP-T.

- A working (establishing a link) SFT-P can have up to 65 °C/140 °F in temperature. Do not touch it when working or immediately after stopping to prevent getting burned.

Caution. Hot! (all sides)



- To remove an SFP-T, follow the following procedures. Otherwise, you may get burned.
- To remove an SFP-T without turning off the device, execute the `inactivate` command, and remove the SFP-T five minutes later.
- To remove an SFP-T from the device turned off, power off the switch of the device, and remove the SFP-T five minutes later.
- An SFP-T has the following label attached.



■ Lithium battery

- This device mounts a lithium battery for the real-time clock. If the lithium battery is inadvertently handled, a personal injury or fire may be caused as a result of heat generation, burst, or ignition. Do not remove the lithium battery from the device or disassemble it, heat it to 100 °C/212 °F or higher, burn it, or wet it with water.

■ Cleaning

- Remove dust on and around the device on a regular basis. Device shutdown and fire disasters or electric shock may be caused.

CAUTION

- **Do not power off the device during software update (when the `ppupdate` command is being executed).**
 - By the execution of the `ppupdate` command, the device automatically restarts. Do not power off the device during restart (until the STATUS LED on the basic control unit changes from blinking in green into steady light). The device may be damaged.

- **Handle a memory card with care.**
 - Do not forcibly push or flip a memory card to insert. Do not forcibly pull out a locked memory card to remove. Otherwise, the connector of the memory card slot may be damaged.
 - Remove the memory card to reposition the device. Moving the device may cause force against the memory card, which can damage the connector of the memory card slot.

- **Do not remove the memory card or disconnect power while the ACC LED is lit.**
 - Lighting of the ACC LED on the basic control unit indicates that the memory card is being accessed. Do not remove the memory card or disconnect power during access. The memory card may be damaged. Some commands require a considerable time before completing access to the memory card after the entry of the commands. Ensure that access is completed and then remove the memory card or disconnect power.

- **Do not attach a label or the like to the transceivers.**
 - The transceiver has a label indicating its manufacturer and that it is our standard supply. However, this label is attached to the part that does not obstruct heat radiation from the transceiver or the mechanism preventing slip-off from the cage. If a label or the like is attached to such an obstructing part, the transceiver or the network interface module may be damaged.

- **For the power supply equipment, considerations must be given not to cause voltage drop due to rush current.**
 - When this device is powered on, a rush current flows. Considerations must be given not to cause voltage drop due to such a rush current. The voltage drop affects not only this device but other devices connected to the same power supply equipment.

- **When installing/uninstalling the power cable, turn off the power switch.**
 - To install or uninstall the power cable, turn off the switch on the power supply to be installed or uninstalled.

- **When replacing the fan unit while the device powered on, complete the task within the specified duration of time.**
 - When replacing the fan unit while the device powered on, complete the entire task from removal to installation within one minute. If it takes more than one minute, other modules may be affected by temperature rise in the device.

■ For carrying or packaging the device and optional component, use an antistatic wrist strap.

- Use an antistatic wrist strap. If you handle the device without the antistatic wrist strap, the device can be damaged by the static electricity.

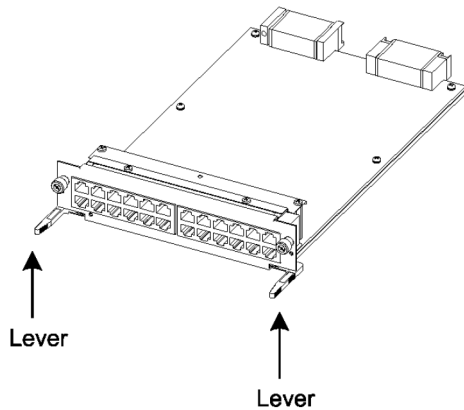
■ After removing an optional component, be sure to attach a blank panel.

- After removing an optional component, be sure to attach a blank panel. Using the device without the blank panel attached, the air flow in the device cannot be maintained. In such a case, the temperature rise inside the device may cause a failure.

■ Attach an option component with care.

- Follow the following procedures to attach an option component. Otherwise, a problem may occur on the device.

1. Open the levers as the figure below.



2. With the levers in hands, push the component slowly into the device, to the point where the levers touch the device.
3. Use the levers to insert the component all the way. Move the levers slowly (taking more than one second) but not forcedly.

■ Before removing an optional component, loosen the screws completely.

- Use levers to remove the basic control unit, basic switching unit or network interface module. If screws are not completely loosened, the optional component may be damaged when the levers are pressed down.

■ When carrying or packing an optional component, take care for handling.

- Take care not to handle the connector when carrying or packing optional components such as the basic control unit, basic switching unit, network interface module, memory card, transceiver, and power supply. They must be stored in antistatic bags when they are not in use.

■ Do not install the device in any place possibly reaching a high temperature.

- Be careful that the parts may be damaged if left in a place exposed to direct sunlight or close to a heating apparatus.

■ Do not bring a TV or radio close to the device.

- Leaving a TV or radio close to the device can adversely influence to each other. If a TV or radio interferes the device, remedy as follows:
 1. Keep the device from the television or radio set as far away as possible.
 2. Change the direction of the antenna for the television or radio set.
 3. Use different outlets.

■ Keep the device away from a place with hydrogen sulfide or much salt.

- Places with hydrogen sulfide including hot spring resorts, and places with much salt including coasts may shorten lifetime of the device.

■ Use air dusters with care.

- Choose an air duster designated to clean optical connectors. Other air dusters may get the end face of the ferrule dirty.
- Avoid the nozzle or container of an air duster from touching the end face of the ferrule. Otherwise, the ferrule may be damaged.

■ Handle the optical connector with care.

- Use the designated optical connector cleaner. Other optical connector cleaners may get the end face of the ferrule dirty.
- Make sure of no problems on the head part of an optical connector cleaner, including attached fabric, grime, and other foreign substances. Otherwise, the end face of the ferrule may be damaged.
- Do not push the optical connector forcedly to clean. Otherwise, the end face of the ferrule may be damaged.
- Rotate an optical connector cleaner (stick type) only in a clockwise direction. An optical connector cleaner rotating clockwise as well as counterclockwise may damage the end face of the ferrule.

■ Maintenance and cleaning

- Wipe off the dirt on the device's outer surface with a dry, clean cloth or a well-wrung wet cloth containing water or neutral cleanser. Do not apply volatile organic solvents or chemicals including benzine and thinner pre-moistened cloths or insect killers, since they can deform, discolor or damage the device.

■ Long-term downtime

- For a long downtime, such as due to a long vacation or travel, be sure to unplug the power cable from the wall outlet for safety. For a configuration using DC power supply, turn off the breaker on the power facility.

■ Discarding this device

- Discard the device according to the ordinance or rule of the local government or call the local waste material handling facility.



Safety Guide [IP8800/S6600]

■ Safety guide for the IP8800/S6600 series

- This document provides safety-related notices for use of the IP8800/S6600 series. To utilize the functions of this device, read this document completely and carefully before using the device.
- Keep this document at hand after you read it, so that you can always refer it later.
- For any operation, follow the directions and procedures given by this document.
- Observe the cautions labeled on the device or those presented by this document. If you fail to do so, you will cause damage to yourself or the device.

■ Symbols

- We have various symbols displayed on the IP8800/S6600 series and in the manuals to guide you in using the IP8800/S6600 series correctly and safely without injuring yourself and others, or damaging equipment assets. Below are the symbols and their meanings. Fully understand the description and then proceed with reading the main part of the manual.

 WARNING	If you ignore instructions preceded by this symbol, you could cause personal injury or death to yourself and others.
 CAUTION	If you ignore instructions preceded by this symbol, you could cause personal injury to yourself and others, or serious damage to the device or surroundings.
CAUTION	If you ignore instructions preceded by this symbol, you could cause physical damage to the device or surroundings.
NOTE	A note is informational in nature. Unlike warning and caution notices, notes (for prevention of malfunction, prevention of product minor damages) are not related to the physical injury or damage to the device.

■ Operations and actions

- Do not attempt to perform any operations not specifically described in this document.
In case of a problem on the device, contact the maintenance personnel after performing the following.
 - For the device with AC power supply mounted, power off the device and unplug the power cable from the outlet.
 - For the device with DC power supply mounted, power off the device and turn off the breaker in the power supply equipment.

■ Be careful in operation

- The instructions displayed on the device or in this manual are the results of our thorough consideration. However, an unexpected situation may occur. For operations, not only follow the instructions but also always be careful yourself.

 **WARNING**

- **In case a failure should occur, power off the device immediately.**
 - In case fume or unusual odor should occur, or foreign matters should come into the device, power off the device as follows. If the device is used in a faulty state, fire disasters or electric shock may be caused.
 - For the device with AC power supply mounted, power off the device and unplug the power cable from the outlet.
 - For the device with DC power supply mounted, power off the device and turn off the breaker in the power supply equipment because the power cable is connected via a terminal.
- **Do not place the device in an unstable location.**
 - If the device is being placed on a table, be sure to install it horizontally on a workbench or the like that can sufficiently bear the weight of the device. If the device is placed on an unstable location such on a shaky table or slope, the device may fall and drop and consequently personal injury may occur.
- **Do not remove the device cover.**
 - Do not remove the device cover. Electric shock may be caused.
- **Do not put foreign matters in the device.**
 - Do not insert or drop metals or combustibles into the device through the intake/exhaust port. Fire disasters or electric shock may be caused.
- **Modification is not permissible.**
 - Device modification is not permissible. Fire disasters or electric shock may be caused.
- **Do not give a shock.**
 - In case the device is dropped or parts are damaged, power off the device, pull the cable out of the outlet, and call the maintenance engineer. Otherwise it can cause a fire or electric shock.
- **Do not put any material on the device.**
 - Do not put a metal such as pin or clip or a container with water in it such as vase or flower pot on the device. Fire disasters or electric shock may be caused.
- **Do not use power not specified.**
 - Do not use a supply voltage not specified. Fire disasters or electric shock may be caused.
- **The current capacity supplied to the power distribution panel must be larger than the operating current of the breaker.**
 - The current capacity supplied to the power distribution panel must be larger than the operating current of the breaker. Otherwise, the breaker may not work in the event of a failure and cause fire disasters.

■ **Grounding is required.**

- Leak current of up to 3.5mA flows for each device. If connecting the device with AC power, be sure to use the grounded outlet. If the power supply is used without grounding, an electric shock may be caused and failures may occur due to electric noise.
- When the device is connected to the DC power supply, be sure to connect the grounding terminal. If the power supply is used without grounding, an electric shock may be caused and failures may occur due to electric noise.

■ **Installing/uninstalling of the DC power cable must be performed by the trained engineer or maintenance personnel.**

- Installing/uninstalling of the DC power cable must be performed by the trained engineer or maintenance personnel. DC power cable is connected to the power supply via a terminal. Therefore, inadvertent handling of the DC power cable may result in fire disasters or electric shock.

■ **Before installing or removing a DC power cable, turn off the breaker on power supply facilities.**

- Before installing or removing a DC power cable, turn off the breaker on power supply facilities. Operation with the breaker on may cause electric shock.

■ **Attach insulation covers on the 0V and -48V terminals of a DC power cable.**

- Attach insulation covers on the 0V and -48V terminals of a DC power cable (the side of which connects to power supply facilities). Operation without insulation covers may cause electric shock.

■ **When using the DC power supply, do not leave the terminal board uncovered.**

- When using the DC power supply, be sure to attach the cover to the terminal board after connecting the power cable. Operating it without the terminal board cover can cause an electric shock.

■ **Do not touch the potential tap.**

- The power supply is provided with the potential tap. This tap is used for inspection at shipment. Customer should not use this tap. Do not insert a sharp material such as pin or clip into the potential tap. Fire disasters or electric shock may be caused.

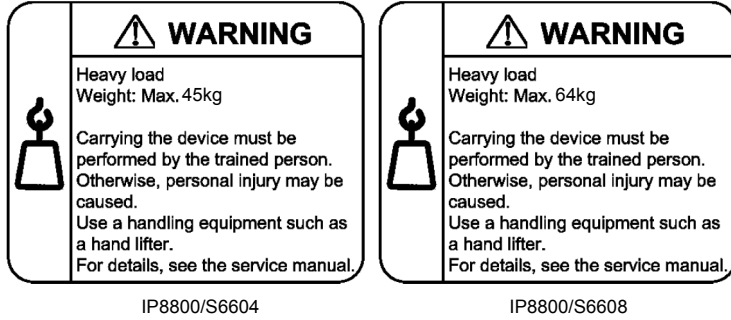
■ **The device must be carried and installed by at least three people.**

- The table below shows mass of the devices. The device must be carried and installed by at least three people. Otherwise, a personal injury due to drop or fall may be caused.

Number of people to carry the device

Model	Mass	Number of people
IP8800/S6604	45 kg/100 lb	3 or more
IP8800/S6608	64 kg/142 lb	

The label below is attached to the device.



■ Handle the power cable with caution.

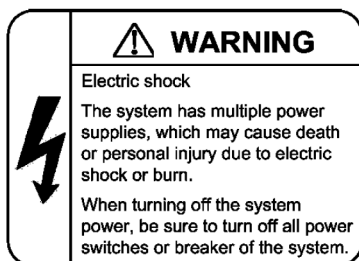
- Do not put a heavy material on the power cable or do not pull, bend, or modify the power cable. The power cable will be damaged and fire disasters or electric shock may be caused. A heavy material may be placed as a result of covering the cable with a floor carpet.
- Use the attached power cable or the power cable complying with the specifications. If any other cable is used, fire disasters or electric shock may be caused. Do not use the attached power cable for other purposes. In such a case, fire disasters or electric shock may be caused.
- If the power cable is degraded (e.g., wire cores exposed or broken), ask the service personnel for replacement. Otherwise it can cause a fire or electric shock.
- Check to see if dust is deposited on the power plug. Insert the plug securely to the end so that shakiness will not occur. If dust is deposited or connection is incomplete, fire disasters or electric shock may be caused.

■ Do not plug too many leads into a single outlet.

- Do not plug too many power plugs into a single outlet. Many loads on an electrical outlet may result in fire disasters and the electric energy in use may be exceeded, the breaker may go off, and other components may be affected.

■ Before powering off, turn off all power switches or breakers on the device.

- Multiple input power supplies are provided to the device. Before powering off, turn off all power switches (when AC power supply is mounted) or breakers (when DC power supply is mounted) on the device. The label below is attached to the device.



- **Work to add or replace equipment must be performed by a trained engineer or maintenance personnel.**
 - To add or replace optional components must be performed by a trained engineer or maintenance personnel. To add or replace a power supply involves to plug and unplug power cables; a person other than the preceding ones may fail to handle things, which can cause fire disaster, electric shock, and equipment failure. Other optional components, if handled mistakenly, can also cause fire disaster, wounds, and equipment failure.

- **Do not press the switch on the basic control unit with a fragile tip, pin, or clip that may get stuck and cannot be removed.**
 - Do not press the switch on the front panel of the basic control unit with a fragile tip, pin, or clip that may get stuck and cannot be removed. Fire disasters or electric shock may be caused.

- **Before addition or replacement of the power supply, unplug the power cable.**
 - Remove the power cable from the power supply when adding or replacing it. With the power cable connected, the power supply equipment may remain energized from some circuits even the power switch is turned off. Therefore, adding or replacing the power supply with the power cable connected may cause a fire or electric shock.

- **Keep air dusters away from fire.**
 - If you use an air duster with combustible gas to clean the optical connector, keep away from fire. Otherwise, fire disaster may occur.

CAUTION

■ **Do not install the device in a humid or dusty environment.**

- Do not install the device in a humid or dusty environment. Fire disasters or electric shock may be caused.
- Moving the device from a cold place to a warm place may form condensation on the surface or internal of the device. If the device is operated immediately a fire or electric shock can be caused. Thus, in this case, leave the device as it is for several hours before starting operation.

■ **Do not stack the devices.**

- Do not stack the devices. The device may be damaged. The device may be damaged or lose its balance and fall or drop. As a result, personal injury may occur.

■ **Do not recline on the device, or place a heavy loading on it.**

- Do not ride on or cling to the device or do not put a heavy material on it. The device may be damaged. The device may be damaged or lose its balance and fall or drop. As a result, personal injury may occur.

■ **When installing the device on the rack, use brackets to support the weight of the device.**

- The rack-attaching brackets supplied with this device are used to fasten the device on the rack but not to support the weight of the device. Use either of the following.

Model	Items
IP8800/S6604	guide rail, shelf, support brackets
IP8800/S6608	guide rail, shelf

The guide rail or shelf, if you use, must be the one attached to the rack and capable of supporting the weight of the fully mounted device.

■ **Use support brackets only for IP8800/S6604.**

- The support brackets support only IP8800/S6604. Do not use for others. Otherwise, the equipment may fall or drop and damage you.

■ **Use support brackets with care.**

- When you mount the device on a rack with support brackets, support the device flatly from both front and rear sides while mounting the device and fastening screws. A tilted device may fall or drop and damage you and other equipment mounted on the same rack.
- To mount the device on a rack with support brackets means weight of the device is supported only by rack-attaching brackets and the support brackets. Make sure to fasten screws of the rack-attaching brackets and the support brackets tightly.

■ **Do not block the intake and/or exhaust port.**

- Do not block the intake/exhaust port of the device. Blocking the intake/exhaust port keeps heat inside and fire disasters may be caused. Keep a space of at least 70mm from the intake/exhaust port.

■ **Do not bring hairs or any foreign matters close to the intake/exhaust port of the device.**

- The cooling fan unit is provided on the device. Do not put any material close to the intake/exhaust port. The internal temperature rise may result in a failure. Do not put hair or any material close to the intake/exhaust port. You may be caught and injured.

■ **When moving an optional component, do not carry it by holding its handle.**

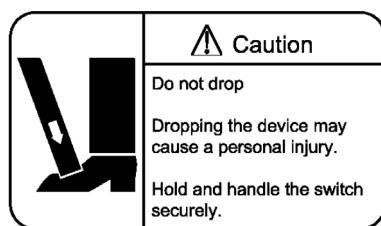
- When moving a fan unit or power supply, do not hold its handle. The handle may come off and the device may drop. As a result, a personal injury may occur. Or the fan unit or power supply may be deformed that may cause a fire or electric shock.

■ **Before carrying the device, remove the cables.**

- When moving the device, power off the device, remove all the cables from the device, and then move the device. Otherwise the device or cable may be deformed or damaged. As a result, fire disasters or electric shock may be caused.

■ **Do not drop an optional component.**

- Handle the optional component carefully not to drop it. If dropped, personal injury may be caused.
- The weight and depth of the DC power supply are 5.6kg and 163mm respectively. When removing the DC power supply, hold it securely. If pulling it forward carelessly, it may drop and cause a personal injury. The label below is attached to the DC power supply.



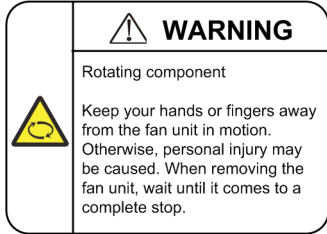
■ **Do not touch the inside of the device.**

- Do not put your hand inadvertently inside the device. Mechanical parts may cause a personal injury.

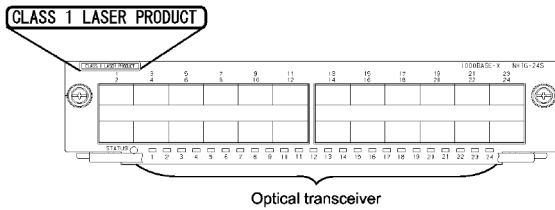
■ **The basic switching unit and network interface component may be hot. Be careful when removing them.**

- Parts mounted on the basic switching unit and network interface component may be hot: Do not touch them to prevent getting burned.

- When removing the fan unit, do not put your hand close to the rotating fan.
 - The fan may still be rotating immediately after the removal of the fan unit. While the fan is rotating, do not put your hand or finger close to it. Personal injury may be caused. The label below is attached to the fan unit.



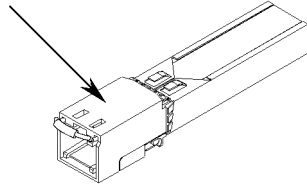
- Do not roughly handle the power cable.
 - Do not put the power cable close to the heating apparatus. The cable sheath may be melted and fire disasters or electric shock may be caused.
 - When inserting the power cable into the outlet or removing from it, be sure to hold the cable plug. Pulling up the cable with the cable grasped, the wire can be broken.
- Do not touch the device directly if you have metal allergies.
 - This device is coated with metals including zinc, nickel, and gold. If you have allergies to them, do not touch the device directly to prevent getting dermatitis.
- Be careful of laser beams.
 - The network interface module as indicated below uses laser beams. Do not peep in the optical transceiver directly.



■ Do not touch a working (including immediately after stopping) SFP-T.

- A working (establishing a link) SFP-T can have up to 65 °C/140 °F in temperature. Do not touch it when working or immediately after stopping to prevent getting burned.

Caution. Hot! (all sides)



- To remove an SFP-T, follow the following procedures. Otherwise, you may get burned.
 - To remove an SFP-T without turning off the device, execute the `inactivate` command, and remove the SFP-T five minutes later.
 - To remove an SFP-T from the device turned off, power off the switch of the device, and remove the SFP-T five minutes later.
- An SFP-T has the following label attached.



■ Lithium battery

- This device mounts a lithium battery for the real-time clock. If the lithium battery is inadvertently handled, a personal injury or fire may be caused as a result of heat generation, burst, or ignition. Do not remove the lithium battery from the device or disassemble it, heat it to 100 °C/212 °F or higher, burn it, or wet it with water.

■ Cleaning

- Remove dust on and around the device on a regular basis. Device shutdown and fire disasters or electric shock may be caused.

CAUTION

■ Do not power off the device during software update (when the `ppupdate` command is being executed).

- By the execution of the `ppupdate` command, the device automatically restarts. Do not power off the device during restart (until the STATUS LED on the control switching unit changes from blinking in green into steady light). The device may be damaged.

■ Handle a memory card with care.

- Do not forcibly push or flip a memory card to insert. Do not forcibly pull out a locked memory card to remove. Otherwise, the connector of the memory card slot may be damaged.
- Remove a memory card to reposition the device. Moving the device may cause force against the memory card, which can damage the connector of the memory card slot.

■ Do not remove the memory card or disconnect power while the ACC LED is lit.

- Lighting of the ACC LED on the basic switching unit indicates that the memory card is being accessed. Do not remove the memory card or disconnect power during access. The memory card may be damaged. Some commands require a considerable time before completing access to the memory card after the entry of the commands. Ensure that access is completed and then remove the memory card or disconnect power.

■ Do not attach a label or the like to the transceivers.

- The transceiver has a label indicating its manufacturer and that it is our standard supply. However, this label is attached to the part that does not obstruct heat radiation from the transceiver or the mechanism preventing slip-off from the cage. If a label or the like is attached to such an obstructing part, the transceiver or the network interface module may be damaged.

■ For the power supply equipment, considerations must be given not to cause voltage drop due to rush current.

- When this device is powered on, a rush current flows. Considerations must be given not to cause voltage drop due to such a rush current. The voltage drop affects not only this device but other devices connected to the same power supply equipment.

■ When installing/uninstalling the power cable, turn off the power switch.

- To install or uninstall the power cable, turn off the switch on the power supply to be installed or uninstalled.

■ When replacing the fan unit while the device powered on, complete the task within the specified duration of time.

- When replacing the fan unit while the device powered on, complete the entire task from removal to installation within one minute. If it takes more than one minute, other modules may be affected by temperature rise in the device.

■ For carrying or packaging the device and optional component, use an antistatic wrist strap.

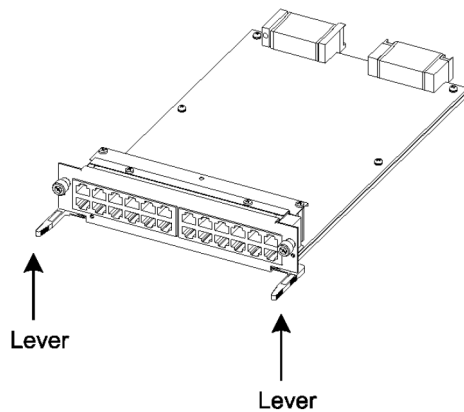
- Use an antistatic wrist strap. If you handle the device without the antistatic wrist strap, the device can be damaged by the static electricity.

■ After removing an optional component, be sure to attach a blank panel.

- After removing an optional component, be sure to attach a blank panel. Using the device without the blank panel attached, the air flow in the device cannot be maintained. In such a case, the temperature rise inside the device may cause a failure.

■ Attach an option component with care.

- Follow the following procedures to attach an option component. Otherwise, a problem may occur on the device.
1. Open the levers as the figure below.



2. With the levers in hands, push the component slowly into the device, to the point where the levers touch the device.
3. Use the levers to insert the component all the way. Move the levers slowly (taking more than one second) but not forcedly.

■ Before removing an optional component, loosen the screws completely.

- Use levers to remove the basic switching unit or network interface module. If screws are not completely loosened, the optional component may be damaged when the levers are pressed down.

■ When carrying or packing an optional component, take care for handling.

- Take care not to handle the connector when carrying or packing optional components such as the basic switching unit, network interface module, memory card, transceiver, and power supply. They must be stored in antistatic bags when they are not in use.

■ Do not install the device in any place possibly reaching a high temperature.

- Be careful that the parts may be damaged if left in a place exposed to direct sunlight or close to a heating apparatus.

■ **Do not bring a TV or radio close to the device.**

- Leaving a TV or radio close to the device can adversely influence to each other. If a TV or radio interferes the device, remedy as follows:
 1. Keep the device from the television or radio set as far away as possible.
 2. Change the direction of the antenna for the television or radio set.
 3. Use different outlets.

■ **Keep the device away from a place with hydrogen sulfide or much salt.**

- Places with hydrogen sulfide including hot spring resorts, and places with much salt including coasts may shorten lifetime of the device.

■ **Use air dusters with care.**

- Choose an air duster designated to clean optical connectors. Other air dusters may get the end face of the ferrule dirty.
- Avoid the nozzle or container of an air duster from touching the end face of the ferrule. Otherwise, the ferrule may be damaged.

■ **Handle the optical connector with care.**

- Use the designated optical connector cleaner. Other optical connector cleaners may get the end face of the ferrule dirty.
- Make sure of no problems on the head part of an optical connector cleaner, including attached fabric, grime, and other foreign substances. Otherwise, the end face of the ferrule may be damaged.
- Do not push the optical connector forcedly to clean. Otherwise, the end face of the ferrule may be damaged.
- Rotate an optical connector cleaner (stick type) only in a clockwise direction. An optical connector cleaner rotating clockwise as well as counterclockwise may damage the end face of the ferrule.

■ **Maintenance and cleaning**

- Wipe off the dirt on the device's outer surface with a dry, clean cloth or a well-wrung wet cloth containing water or neutral cleanser. Do not apply volatile organic solvents or chemicals including benzine and thinner pre-moistened cloths or insect killers, since they can deform, discolor or damage the device.

■ **Long-term downtime**

- For a long downtime, such as due to a long vacation or travel, be sure to unplug the power cable from the wall outlet for safety. For a configuration using DC power supply, turn off the breaker on the power facility.

■ **Discarding this device**

- Discard the device according to the ordinance or rule of the local government or call the local waste material handling facility.



Safety Guide [IP8800/S6300]

■ Safety guide for the IP8800/S6300 series

- This document provides safety-related notices for use of the IP8800/S6300 series. Read this document completely and carefully before using the device.
- Keep this document at hand after you read it, so that you can always refer it later.
- For any operation, follow the directions and procedures given by this document.
- Observe the cautions labeled on the device or those presented by this document. If you fail to do so, you will cause damage to yourself or the device.

■ Symbols

- We have various symbols displayed on the IP8800/S6300 series and in the manuals to guide you in using the IP8800/S6300 series correctly and safely without injuring yourself and others, or damaging equipment assets. Below are the symbols and their meanings. Fully understand the description and then proceed with reading the main part of the manual.

 WARNING	If you ignore instructions preceded by this symbol, you could cause personal injury or death to yourself and others.
 CAUTION	If you ignore instructions preceded by this symbol, you could cause personal injury to yourself and others, or serious damage to the device or surroundings.
CAUTION	If you ignore instructions preceded by this symbol, you could cause physical damage to the device or surroundings.
NOTE	A note is informational in nature. Unlike warning and caution notices, notes (for prevention of malfunction, prevention of product minor damages) are not related to the physical injury or damage to the device.

■ Operations and actions

- Do not attempt to perform any operations not specifically described in this document.
In case of a problem on the device, contact the maintenance personnel after performing the following.
 - For the device with AC power supply mounted, power off the device and unplug the power cable from the outlet.
 - For the device with DC power supply mounted, power off the device and turn off the breaker in the power supply equipment.

■ Be careful in operation

The instructions displayed on the device or in this manual are the results of our thorough consideration.

- However, an unexpected situation may occur. For operations, not only follow the instructions but also always be careful yourself.

 **WARNING**

- **In case a failure should occur, power off the device immediately.**
 - In case fume or unusual odor should occur, or foreign matters should come into the device, power off the device as follows. If the device is used in a faulty state, fire disasters or electric shock may be caused.
 - For the device with AC power supply mounted, power off the device and unplug the power cable from the outlet.
 - For the device with DC power supply mounted, power off the device and turn off the breaker in the power supply equipment because the power cable is connected via a terminal.

- **Do not place the device in an unstable location.**
 - If the device is being placed on a table, be sure to install it horizontally on a workbench or the like that can sufficiently bear the weight of the device. If the device is placed on an unstable location such on a shaky table or slope, the device may fall and drop and consequently personal injury may occur.

- **Do not remove the device cover.**
 - Do not remove the device cover. Electric shock may be caused.

- **Do not put foreign matters in the device.**
 - Do not insert or drop metals or combustibles into the device through the intake/exhaust port. Fire disasters or electric shock may be caused.

- **Modification is not permissible.**
 - Device modification is not permissible. Fire disasters or electric shock may be caused.

- **Do not give a shock.**
 - In case the device is dropped or parts are damaged, power off the device, pull the cable out of the outlet, and call the maintenance engineer. Otherwise it can cause a fire or electric shock.

- **Do not put any material on the device.**
 - Do not put a metal such as pin or clip or a container with water in it such as vase or flower pot on the device. Fire disasters or electric shock may be caused.

- **Do not use power not specified.**
 - Do not use a supply voltage not specified. Fire disasters or electric shock may be caused.

- **The current capacity supplied to the power distribution panel must be larger than the operating current of the breaker.**
 - The current capacity supplied to the power distribution panel must be larger than the operating current of the breaker. Otherwise, the breaker may not work in the event of a failure and cause fire disasters.

■ Grounding is required.

- Leak current of up to 3.5mA flows for each device. For connecting to the AC power supply, be sure to use the grounded outlet. If the power supply is used without grounding, an electric shock may be caused and failures may occur due to electric noise.
- For connecting the DC power supply, be sure to connect the grounding terminal. If the power supply is used without grounding, an electric shock may be caused and failures may occur due to electric noise.

■ Installing/uninstalling of the DC power cable must be performed by the trained engineer or maintenance personnel.

- Installing/uninstalling of the DC power cable must be performed by the trained engineer or maintenance personnel. DC power cable is connected to the power supply via a terminal. Therefore, inadvertent handling of the DC power cable may result in fire disasters or electric shock.

■ Before installing or removing a DC power cable, turn off the breaker on power supply facilities.

- Before installing or removing a DC power cable, turn off the breaker on power supply facilities. Operation with the breaker on may cause electric shock.

■ Attach insulation covers on the 0V and -48V terminals of a DC power cable.

- Attach insulation covers on the 0V and -48V terminals of a DC power cable (the side of which connects to power supply facilities). Operation without insulation covers may cause electric shock.

■ When using the DC power supply, do not leave the terminal board uncovered.

- When using the DC power supply, be sure to attach the cover to the terminal board after connecting the power cable. Operating it without the terminal board cover can cause an electric shock.

■ Do not touch the potential tap.

- The power supply is provided with the potential tap. However, this tap is used for inspection at shipment. Customer should not use this tap. Do not insert a sharp material such as pin or clip into the potential tap. Fire disasters or electric shock may be caused.

■ The device must be carried and installed by at least three people.

- The table below shows mass of the devices. The device must be carried and installed by at least three people. Otherwise, a personal injury due to drop or fall may be caused.

Number of people to carry the device

Model	Mass	Number of people
IP8800/S6304	45kg/100 lb	3 or more
IP8800/S6308	64kg/142 lb	

The label below is attached to the device.



IP8800/S6304



IP8800/S6308

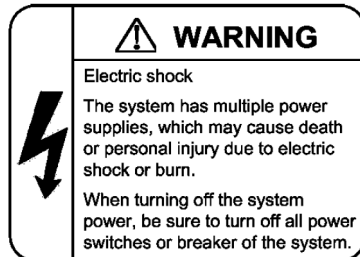
■ Handle the power cable with caution.

- Do not put a heavy material on the power cable or do not pull, bend, or modify the power cable. The power cable will be damaged and fire disasters or electric shock may be caused. A heavy material may be placed as a result of covering the cable with a floor carpet.
- Use the attached power cable or the power cable complying with the specifications. If any other cable is used, fire disasters or electric shock may be caused. Do not use the attached power cable for other purposes. In such a case, fire disasters or electric shock may be caused.
- If the power cable is degraded (e.g., wire cores exposed or broken), ask the service personnel for replacement. Otherwise it can cause a fire or electric shock.
- Check to see if dust is deposited on the power plug. Insert the plug securely to the end so that shakiness will not occur. If dust is deposited or connection is incomplete, fire disasters or electric shock may be caused.

■ Do not plug too many leads into a single outlet.

- Do not plug too many power plugs into a single outlet. Many loads on an electrical outlet may result in fire disasters and the electric energy in use may be exceeded, the breaker may go off, and other components may be affected.

- Before powering off, turn off all power switches or breakers on the device.
 - Multiple input power supplies are provided to the device. Before powering off, turn off all power switches (when AC power supply is mounted) or breakers (when DC power supply is mounted) on the device. The label below is attached to the device.



- Work to add or replace equipment must be performed by a trained engineer or maintenance personnel.
 - To add or replace optional components must be performed by a trained engineer or maintenance personnel. To add or replace a power supply involves to plug and unplug power cables; a person other than the preceding ones may fail to handle things, which can cause fire disaster, electric shock, and equipment failure. Other optional components, if handled mistakenly, can also cause fire disaster, wounds, and equipment failure.
- Do not press the switch on the front panel of the management and switching unit with a fragile tip, pin, or clip that may get stuck and cannot be removed.
 - Do not press the switch on the front panel of the management and switching unit with a fragile tip, pin, or clip that may get stuck and cannot be removed. Fire disasters or electric shock may be caused.
- Before addition or replacement of the power supply, unplug the power cable.
 - Remove the power cable from the power supply when adding or replacing it. With the power cable connected, the power supply equipment may remain energized from some circuits even the power switch is turned off. Therefore, adding or replacing the power supply with the power cable connected may cause a fire or electric shock.
- Keep air dusters away from fire.
 - If you use an air duster with combustible gas to clean the optical connector, keep away from fire. Otherwise, fire disaster may occur.

CAUTION

■ **Do not install the device in a humid or dusty environment.**

- Do not install the device in a humid or dusty environment. Fire disasters or electric shock may be caused.
- Moving the device from a cold place to a warm place may form condensation on the surface or internal of the device. If the device is operated immediately a fire or electric shock can be caused. Thus, in this case, leave the device as it is for several hours before starting operation.

■ **Do not stack the devices.**

- Do not stack the devices. The device may be damaged. The device may be damaged or lose its balance and fall or drop. As a result, personal injury may occur.

■ **Do not recline on the device, or place a heavy loading on it.**

- Do not ride on or cling to the device or do not put a heavy material on it. The device may be damaged. The device may be damaged or lose its balance and fall or drop. As a result, personal injury may occur.

■ **When installing the device on the rack, use brackets to support the weight of the device.**

- The rack-attaching brackets supplied with this device are used to fasten the device on the rack but not to support the weight of the device. Use either of the following.

Model	Items
IP8800/S6304	guide rail, shelf, support brackets
IP8800/S6308	guide rail, shelf

The guide rail or shelf, if you use, must be the one attached to the rack and capable of supporting the weight of the fully mounted device.

■ **Use support brackets only for IP8800/S6304.**

- The support brackets support only IP8800/S6304. Do not use for others. Otherwise, the equipment may fall or drop and damage you.

■ **Use support brackets with care.**

- When you mount the device on a rack with support brackets, support the device flatly from both front and rear sides while mounting the device and fastening screws. A tilted device may fall or drop and damage you and other equipment mounted on the same rack.
- To mount the device on a rack with support brackets means weight of the device is supported only by rack-attaching brackets and the support brackets. Make sure to fasten screws of the rack-attaching brackets and the support brackets tightly.

■ **Do not block the intake and/or exhaust port.**

- Do not block the intake/exhaust port of the device. Blocking the intake/exhaust port keeps heat inside and fire disasters may be caused. Keep a space of at least 70mm/2.8 in from the intake/exhaust port.

■ **Do not bring hairs or any foreign matters close to the intake/exhaust port of the device.**

- The cooling fan unit is provided on the device. Do not put any material close to the intake/exhaust port. The internal temperature rise may result in a failure. Do not put hair or any material close to the intake/exhaust port. You may be caught and injured.

■ **When moving an optional component, do not carry it by holding its handle.**

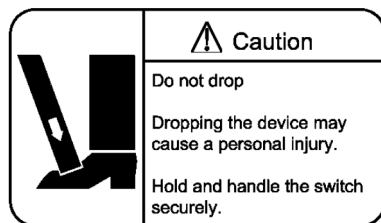
- When moving a fan unit or power supply, do not hold its handle. The handle may come off and the device may drop. As a result, a personal injury may occur. Or the fan unit or power supply may be deformed that may cause a fire or electric shock.

■ **Before carrying the device, remove the cables.**

- When moving the device, power off the device, remove all the cables from the device, and then move the device. Otherwise the device or cable may be deformed or damaged. As a result, fire disasters or electric shock may be caused.

■ **Do not drop an optional component.**

- Handle the optional component carefully not to drop it. If dropped, personal injury may be caused.
- The weight and depth of the DC power supply are 5.6 kg/12.4 lb and 163 mm/6.4 in respectively. When removing the DC power supply, hold it securely. If pulling it forward carelessly, it may drop and cause a personal injury. The label below is attached to the DC power supply.



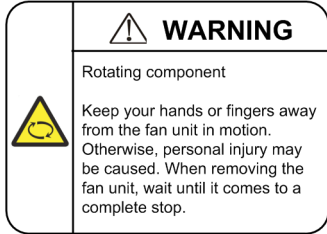
■ **Do not touch the inside of the device.**

- Do not put your hand inadvertently inside the device. Mechanical parts may cause a personal injury.

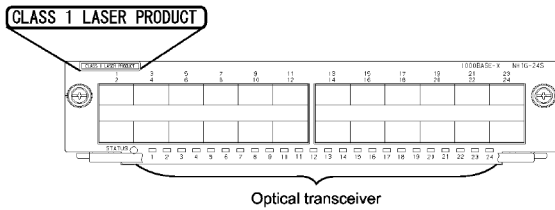
■ **The basic switching unit and network interface component may be hot. Be careful when removing them.**

- Parts mounted on the basic switching unit and network interface component may be hot: Do not touch them to prevent getting burned.

- When removing the fan unit, do not put your hand close to the rotating fan.
 - The fan may still be rotating immediately after the removal of the fan unit. While the fan is rotating, do not put your hand or finger close to it. Personal injury may be caused. The label below is attached to the fan unit.



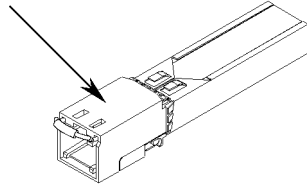
- Do not roughly handle the power cable.
 - Do not put the power cable close to the heating apparatus. The cable sheath may be melted and fire disasters or electric shock may be caused.
 - When inserting the power cable into the outlet or removing from it, be sure to hold the cable plug. Pulling up the cable with the cable grasped, the wire can be broken.
- Do not touch the device directly if you have metal allergies.
 - This device is coated with metals including zinc, nickel, and gold. If you have allergies to them, do not touch the device directly to prevent getting dermatitis.
- Be careful of laser beams.
 - The network interface module as indicated below uses laser beams. Do not peep in the optical transceiver directly.



■ Do not touch a working (including immediately after stopping) SFP-T.

- A working (establishing a link) SFP-T can have up to 65 °C/140 °F in temperature. Do not touch it when working or immediately after stopping to prevent getting burned.

Caution. Hot! (all sides)



- To remove an SFP-T, follow the following procedures. Otherwise, you may get burned.
 - To remove an SFP-T without turning off the device, execute the `inactivate` command, and remove the SFP-T five minutes later.
 - To remove an SFP-T from the device turned off, power off the switch of the device, and remove the SFP-T five minutes later.
- An SFP-T has the following label attached.



■ Lithium battery

- This device mounts a lithium battery for the real-time clock. If the lithium battery is inadvertently handled, a personal injury or fire may be caused as a result of heat generation, burst, or ignition. Do not remove the lithium battery from the device or disassemble it, heat it to 100 °C/212 °F or higher, burn it, or wet it with water.

■ Cleaning

- Remove dust on and around the device on a regular basis. Device shutdown and fire disasters or electric shock may be caused.

CAUTION

■ Do not power off the device during software update (when the `ppupdate` command is being executed).

- By the execution of the `ppupdate` command, the device automatically restarts. Never power off the device during restart (until the STATUS LED on the management and switching unit changes from blinking in green into steady light). The device may be damaged.

■ Handle a memory card with care.

- Do not forcibly push or flip a memory card to insert. Do not forcibly pull out a locked memory card to remove. Otherwise, the connector of the memory card slot may be damaged.
- Remove a memory card to reposition the device. Moving the device may cause force against the memory card, which can damage the connector of the memory card slot.

■ Do not remove the memory card or disconnect power while the ACC LED is lit.

- Lighting of the ACC LED on the management and switching unit indicates that the memory card is being accessed. Do not remove the memory card or disconnect power during access. The memory card may be damaged. Some commands require a considerable time before completing access to the memory card after the entry of the commands. Ensure that access is completed and then remove the memory card or disconnect power.

■ Do not attach a label or the like to the transceivers.

- The transceiver has a label indicating its manufacturer and that it is our standard supply. However, this label is attached to the part that does not obstruct heat radiation from the transceiver or the mechanism preventing slip-off from the cage. If a label or the like is attached to such an obstructing part, the transceiver or the network interface module may be damaged.

■ When installing/uninstalling the power cable, turn off the power switch.

- To install or uninstall the power cable, turn off the switch on the power supply to be installed or uninstalled.

■ When installing/uninstalling the power cable, turn off the power switch.

- To install or uninstall the power cable, turn off the switch on the power supply to be installed or uninstalled.

■ When replacing the fan unit while the device powered on, complete the task within the specified duration of time.

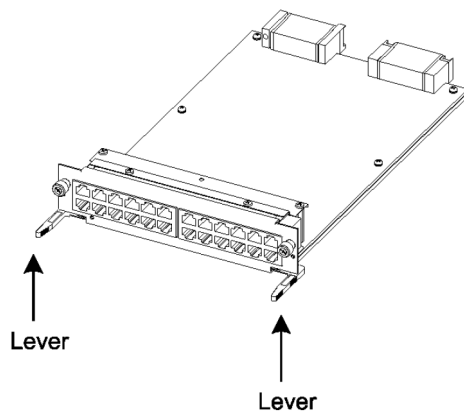
- When replacing the fan unit while the device powered on, complete the entire task from removal to installation within one minute. If it takes more than one minute, other modules may be affected by temperature rise in the device.

■ For carrying or packaging the device and optional component, use an antistatic wrist strap.

- Use an antistatic wrist strap. If you handle the device without the antistatic wrist strap, the device can be

damaged by the static electricity.

- **After removing an optional component, be sure to attach a blank panel.**
 - After removing an optional component, be sure to attach a blank panel. Using the device without the blank panel attached, the air flow in the device cannot be maintained. In such a case, the temperature rise inside the device may cause a failure.
 - **Be sure to install the network interface module with the tray attached.**
 - Be sure to install the network interface module (NIF) with the tray attached to the device. If the NIF is inserted without the tray attached, the connector of the NIF may not fit the connector of the switch, and the connectors of both side may be damaged.
 - **Attach an option component with care.**
 - Follow the following procedures to attach an option component. Otherwise, a problem may occur on the device.
1. Open the levers as the figure below.



2. With the levers in hands, push the component slowly into the device, to the point where the levers touch the device.
 3. Use the levers to insert the component all the way. Move the levers slowly (taking more than one second) but not forcedly.
- **Before removing an optional component, loosen the screws completely.**
 - Use levers to remove the management and switching unit or network interface module. If screws are not completely loosened, the optional component may be damaged when the levers are pressed down.
 - **When carrying or packing an optional component, take care for handling.**
 - Take care not to handle the connector when carrying or packing optional components such as the management and switching unit, network interface module, memory card, transceiver, and power supply. They must be stored in antistatic bags when they are not in use.
 - **Do not install the device in any place possibly reaching a high temperature.**
 - Be careful that the parts may be damaged if left in a place exposed to direct sunlight or close to a heating apparatus.

■ **Do not bring a TV or radio close to the device.**

- Leaving a TV or radio close to the device can adversely influence to each other. If a TV or radio interferes the device, remedy as follows:

1. Keep the device from the television or radio set as far away as possible.
2. Change the direction of the antenna for the television or radio set.
3. Use different outlets.

■ **Keep the device away from a place with hydrogen sulfide or much salt.**

- Places with hydrogen sulfide including hot spring resorts, and places with much salt including coasts may shorten lifetime of the device.

■ **Use air dusters with care.**

- Choose an air duster designated to clean optical connectors. Other air dusters may get the end face of the ferrule dirty.
- Avoid the nozzle or container of an air duster from touching the end face of the ferrule. Otherwise, the ferrule may be damaged.

■ **Handle the optical connector with care.**

- Use the designated optical connector cleaner. Other optical connector cleaners may get the end face of the ferrule dirty.
- Make sure of no problems on the head part of an optical connector cleaner, including attached fabric, grime, and other foreign substances. Otherwise, the end face of the ferrule may be damaged.
- Do not push the optical connector forcedly to clean. Otherwise, the end face of the ferrule may be damaged.
- Rotate an optical connector cleaner (stick type) only in a clockwise direction. An optical connector cleaner rotating clockwise as well as counterclockwise may damage the end face of the ferrule.

■ **Maintenance and cleaning**

- Wipe off the dirt on the device's outer surface with a dry, clean cloth or a well-wrung wet cloth containing water or neutral cleanser. Do not apply volatile organic solvents or chemicals including benzine and thinner pre-moistened cloths or insect killers, since they can deform, discolor or damage the device.

■ **Long-term downtime**

- For a long downtime, such as due to a long vacation or travel, be sure to unplug the power cable from the wall outlet for safety. For a configuration using DC power supply, turn off the breaker on the power facility.

■ **Discarding this device**

- Discard the device according to the ordinance or rule of the local government or call the local waste material handling facility.



Safety Guide [IP8800/S3600] [IP8800/S2400]

■ Safety guide for the IP8800/S3600 and IP8800/S2400 series

- This document provides safety-related notices for use of the IP8800/S3600 and IP8800/S2400 series. To utilize the functions of this device, read this document completely and carefully before using the device.
- Keep this document at hand after you read it, so that you can always refer it later.
- For any operation, follow the directions and procedures given by this document.
- Observe the cautions labeled on the device or those presented by this document. If you fail to do so, you will cause damage to yourself or the device.

■ Symbols

- We have various symbols displayed on the IP8800/S3600 and IP8800/S2400 series and in the manuals to guide you in using the IP8800/S3600 and IP8800/S2400 series correctly and safely without injuring yourself and others, or damaging equipment assets. Below are the symbols and their meanings. Fully understand the description and then proceed with reading the contents of the manual

	WARNING	If you ignore instructions preceded by this symbol, you could cause personal injury or death to yourself and others.
	CAUTION	If you ignore instructions preceded by this symbol, you could cause personal injury to yourself and others, or serious damage to the device or surroundings.
	CAUTION	If you ignore instructions preceded by this symbol, you could cause physical damage to the device or surroundings.
	NOTE	A note is informational in nature. Unlike warning and caution notices, notes (for prevention of malfunction, prevention of product minor damages) are not related to the physical injury or damage to the device.

■ Operations and Handling

- Do not attempt to perform any operations not specifically described in "IP8800/S3600 IP8800/S2400 series Hardware Installation Guide." In the event of a problem, turn off the power, unplug the power cable, and contact a qualified service technician.

The instructions displayed on the device or in this manual are the results of our thorough consideration. However, an unexpected situation may occur. For operations, not only follow the instructions but also always be careful yourself.

■ Be careful in operation

- The instructions shown on the device or in this manual are the results of our thorough consideration. However, an unexpected situation may occur. For operations, not only follow the instructions but also always be careful with your judge.

WARNING

■ **In case a failure should occur, power off the device immediately.**

- In case a trouble such as smoke or unusual odor should occur or foreign materials or water should come in to the device, power off the device immediately. If the device is used in a faulty state, fire disasters or electric shock may be caused.

Actions to Be Taken When a Trouble Occurs

Device in Trouble		Action to Be Taken
AC power supply model AC power supply (PoE) model	Equipped with no external power unit (EPU)	Power off the device, and unplug the power cable.
	Equipped with the external power unit (EPU)	Power off the device and power module, and unplug both power cables.
DC power supply model		Power off the device, and turn off the breaker on the power supply equipment.
Redundant power supply model	Equipped with AC power supplies	Power off all the power supplies mounted on the device, and unplug the power cables.
	Equipped with DC power supplies	Power off all the power supplies mounted on the device, and turn off the breaker on the power supply equipment.
EPU		Power off the EPU and unplug the power cable.

■ **Do not put foreign materials in the device.**

- Do not insert or drop metals or combustibles into the device through the intake/exhaust port. Fire disasters or electric shock may be caused.

■ **Do not press the RESET switch with a fragile tip, pin, or clip that may get stuck and cannot be removed.**

- Do not press the RESET switch with a fragile tip, pin, or clip that may get stuck and cannot be removed. Fire disasters or electric shock may be caused.

■ **Modification is not permissible.**

- Device modification is not permissible. Fire disasters or electric shock may be caused.

■ **Do not give a shock.**

- In case the device is dropped or parts are damaged, power off the device, unplug the power cable out of the outlet, and call the maintenance engineer. Otherwise, fire disasters or electric shock may be caused.

■ **Do not put any material on the device.**

- Do not put a metal such as pin, clip, or a container with water such as a vase or a flower pot on the device. Fire disasters or electric shock may be caused.

■ **Do not use power not specified.**

- Do not use a supply voltage not specified. Fire disasters or electric shock may be caused.

■ **The current capacity supplied to the power distribution panel must be larger than the operating current of the breaker.**

- The current capacity supplied to the power distribution panel must be larger than the operating current of the breaker. Otherwise, the breaker may not work in the event of a failure and cause fire disasters.

■ **Grounding is required.**

- For the AC power supply model, AC power supply (PoE) model, redundant power supply model (with AC power supplies mounted), and external power unit (EPU), be sure to use a grounded outlet. If the power supply is used without grounding, electric shock may be caused and failures may occur due to electric noise.
- For the DC power supply model and redundant power supply model (with DC power supplies mounted), be sure to use a grounding cable. If the power supply is used without grounding, electric shock may be caused and failures may occur due to electric noise.

■ **Installing/uninstalling of the DC power cable must be performed by the trained engineer or maintenance personnel.**

- Installing/uninstalling of the DC power cable must be performed by the trained engineer or maintenance personnel. DC power cable is connected to the power supply via a terminal. Therefore, inadvertent handling of the DC power cable may result in fire disasters or electric shock.

■ **Before installing or removing a DC power cable, turn off the breaker on power supply facilities.**

- Before installing or removing a DC power cable, turn off the breaker on power supply facilities. Operation with the breaker on may cause electric shock and fire disaster.

■ **Attach insulation covers on the G terminal and -48V terminal of a DC power cable.**

- Attach insulation covers on the G terminal and -48V terminal of a DC power cable (the side of which connects to power supply facilities). Operation without insulation covers may cause electric shock.

■ **Observe the specified margin of length when ripping the power cable sheath.**

- When using the -48VDC power cable for the redundant power supply model, rip the power cable sheath (on the device side) with the margin of 8 to 10 mm (0.3 to 0.4 in)..
If the margin is too small, loose connection or cable disconnection may be caused. On the other hand, too large margin may cause conductor exposure, resulting in electric shock.

■ **Do not use the cable with the protection cap detached.**

- Do not remove protection cap except when connecting the cable. Operating them with the protection cap detached may cause an electric shock.
Since external power supply EPU-B has a high output power, the label below is attached near the external power connector.



■ **Handle the power cable with caution.**

- Do not put a heavy material on the power cable or do not pull, bend, or modify the power cable. The power cable will be damaged and fire disasters or electric shock may be caused. A heavy material may be accidentally placed as a result of covering the cable with a floor carpet.
- Use the attached power cable or the power cable complying with the specifications. If any other cable is used, fire disasters or electric shock may be caused. Do not use the attached power cable for other purposes. If used, fire disasters or electric shock may be caused.
- If the power cable is degraded (e.g., wire cores exposed or broken), ask the service personnel for replacement. Otherwise, fire disasters or electric shock may be caused.
- Check to see if no dust is deposited on the power plug. Insert the plug securely to the end so that shakiness will not occur. If dust is deposited or connection is incomplete, fire disasters or electric shock may be caused.

■ **Do not use too many plugs at a single outlet.**

- Do not use too many power plugs at a single outlet. Much loads on an electrical outlet may cause fire disasters and the breaker gone off due to the exceeded in-use electric energy, affecting other components.

■ **Before installing/uninstalling the power supply, unplug the power cable.**

- Before installing/uninstalling the power supply, unplug the power cable from the power supply. With the power cable connected, some circuit supplies power even though the power switch is turned OFF. Therefore, installing/uninstalling the power supply with the power cable connected may cause a fire disasters or electric shock.

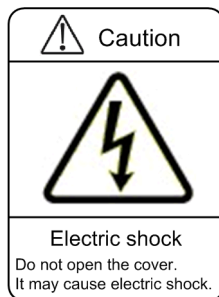
■ **Keep air dusters away from fire.**

- If you use an air duster with combustible gas to clean the optical connector, keep away from fire. Otherwise, fire disaster may occur.

⚠ CAUTION

- **Do not place the device in an unstable location.**
 - If the device is being placed on a table, be sure to install it horizontally on a workbench or the like that can sufficiently bear the weight of the device. If the device is placed on an unstable location such as a shaky table or slope, the device may fall and drop and consequently personal injury may be caused.
 - To mount the device on a rack, make sure that the device is placed in a stable location. If the device is placed in an unstable location, the device may fall and drop and consequently personal injury may be caused.

- **Do not remove the device cover.**
 - Do not remove the device cover. Electric shock may be caused. The label below is attached to the device.



- **Do not block the intake/exhaust port.**
 - Do not block the intake/exhaust port of the device. Blocking the intake/exhaust port keeps heat inside, and fire disasters may be caused. Keep a space of at least 50 mm/2.0 in from the intake/exhaust port.

- **Do not bring hairs or any foreign materials close to the intake/exhaust port of the device.**
 - The cooling fan unit is provided on the device. Do not put any material close to the intake/exhaust port. The internal temperature rise may cause a failure. Do not put hair or any material close to the intake/exhaust port. You may be caught and injured.

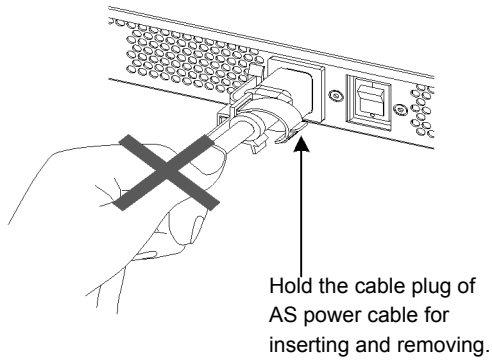
- **When moving the device, do not carry it by holding its handle of power supply, fan unit, or power module.**
 - For the redundant power model, do not carry it by holding its handle of power supply or fan unit when moving the device. The handle may be removed and the device may be dropped. As a result, personal injury may be caused. Also, the device may be deformed and fire disasters or electric shock may be caused.
 - When moving the external power unit (EPU), do not carry it by holding its handle of power module. The handle may be removed and the device may be dropped. As a result, personal injury may be caused. Also, the device may be deformed and fire disasters or electric shock may be caused.

■ Precaution on carrying the device

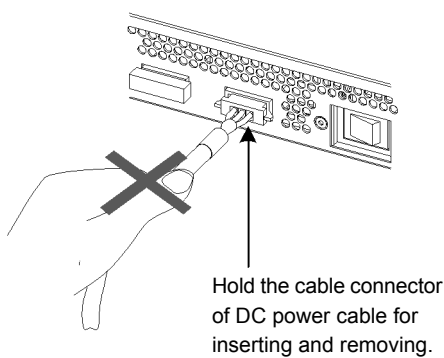
- When moving the device, power off the device, remove the power cable out of the outlet, remove all other cables from the device, and then move the device. Otherwise, the device or cable may be deformed or damaged. As a result, fire disasters or electric shock may be caused.
- When stacking the devices for transportation, put them into package boxes. Otherwise, the device may be deformed or damaged. As a result, fire disasters or electric shock may be caused.

■ Do not roughly handle the power cable.

- Do not put the power cable close to the heating apparatus. The cable sheath may be melted and fire disasters or electric shock may be caused.
- When inserting the AC power cable into the outlet or removing it from the outlet, be sure to hold the cable plug. Pulling up the cable with the cable grasped, the wire can be broken.



- When inserting the DC power cable into the outlet or removing it from the outlet, be sure to hold the cable connector. Pulling up the cable with the cable grasped, the wire can be broken.



■ Shut down all the power to the device before powering off the device.

- For the AC power supply model and AC power supply (PoE) model using the external power unit (EPU), the device cannot be powered off by turning off the power switch on the switch only. To power off, turn off the power switches on the system and the power module.
- When the device has redundant power supply in the redundant power supply model, the device cannot be powered off by turning off the power switch on only one of the power supply equipment. To power off, turn

off the power switches on all power supplies mounted on the device.

■ **Do not touch the device directly if you have metal allergies.**

- This device is coated with metals including zinc, nickel, and gold. If you have allergies to them, do not touch the device directly to prevent getting dermatitis.

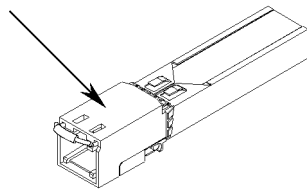
■ **Be careful of the laser beams.**

- The device uses the laser beams, which is invisible, clear and colorless. Do not peep in the optical transceiver directly.

■ **Do not touch a working (including immediately after stopping) SFP-T.**

- A working (establishing a link) SFT-P can have up to 65 °C/140 °F in temperature. Do not touch it when working or immediately after stopping to prevent getting burned.

Caution. Hot! (all sides)



- To remove an SFP-T, follow the following procedures. Otherwise, you may get burned.
- To remove an SFP-T without turning off the device, shut down the SFP slot, and remove the SFP-T five minutes later.
- To remove an SFP-T from the device turned off, power off the switch of the device, and remove the SFP-T five minutes later.
- An SFP-T has the following label attached.



■ **Do not install the device in a humid or dusty environment**

- Do not install the device in a humid or dusty environment. Fire disasters or electric shock may be caused.
- Moving the device from a cold place to a warm place may form condensation on the surface or inside of the device. If the device is operated immediately, a fire or electric shock can be caused. Thus, in this case, leave the device as it is for several hours before starting operation.

■ **Do not touch the inside of the device.**

- Do not put your hand inadvertently inside the device. Mechanical parts may cause personal injury.

■ **Do not ride, recline, or place a heavy loading on the device.**

- Do not ride on or lean against the device. The device may be damaged. Alternatively, the device may lose its balance and fall or drop. As a result, personal injury may be caused.
- Do not put a material weighing over 5 kg/11.1 lb on the device. The device may be damaged. Alternatively, the device may lose its balance and fall or drop. As a result, personal injury may be caused.

■ **Mount the fan unit on the empty slot not to be mounted with a power supply for the redundant power supply model.**

- Be sure to mount the fan unit on the empty slot not to be mounted with a power supply for the redundant power supply model. Using the device without the fan unit, the temperature rise inside the device may cause a failure. If foreign materials enter, a failure may be caused.

■ **Attach a blank panel to the slot on the external power unit (EPU) where the power module is not to be mounted.**

- Be sure to attach a blank panel to the slot on the external power unit (EPU) where the power module is not to be mounted. If the blank panel is not attached, mechanical parts may cause personal injury. If foreign materials enter, a failure may be caused.

■ **Cleaning**

- Remove dust on and around the device on a regular basis. Device shutdown and fire disasters or electric shock may be caused.

CAUTION

- **Do not install the device in any place possibly reaching a high temperature.**
 - Be careful that the parts may be damaged if left in a place exposed to direct sunlight or close to a heating apparatus.

- **Do not bring a TV or radio close to the device.**
 - Leaving a TV or radio close to the device can adversely influence to each other. If the device interferes a TV or radio, remedy as follows:
 - Keep the device from the television or radio set as far away as possible.
 - Change the direction of the antenna for the television or radio set.
 - Use different outlets.

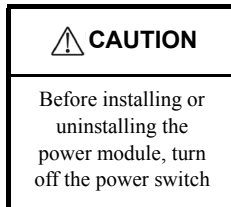
- **Keep the device away from a place with hydrogen sulfide or much salt.**
 - Places with hydrogen sulfide including hot spring resorts, and places with much salt including coasts may shorten lifetime of the device.

- **Before installing/uninstalling the power cable, turn off the power switch.**
 - Before installing/uninstalling the power cables for AC power supply model, PoE AC power supply model, or external power unit (EPU), turn off the power switch on the device.
 - For the redundant power supply model, turn off the power switches on the power supplies before installing or removing the power cable or cable connector.
 - For the external power cable, turn off the power switch on the power module in advance.

- **When replacing the power supply or fan unit with the device powered on, complete the task within the specified duration of time.**
 - When replacing the power supply or fan unit with the device powered on, complete the entire task from removal to installation within three minutes. If it takes more than three minutes, a failure may occur due to temperature rise inside the device.

■ Before installing/uninstalling the power module, turn off the power switch.

- Before installing/uninstalling the power module, turn off the power switch on the power module to be installed or uninstalled. If operation is performed while the power switch on the power module is on, a failure or device trouble may be caused. The label below is attached to the external power unit (EPU)



■ Before turning on the main power switch on the external power unit (EPU), turn off the power switch on the power module.

- Before turning on the main power switch on the external power unit (EPU), turn off the power switch on the every power module mounted.

■ Do not turn off the main power switch on the external power unit (EPU), while the device is backed up by the EPU.

- When turning off the EPU main power switch, the backup power supply to the device is completely shut down. If external power is supplied to the device, do not turn off the main power switch on the EPU.

■ Handle a memory card and a dummy memory card with care.

- Do not forcedly push or flip a (dummy) memory card to insert. Do not forcedly pull out a locked (dummy) memory card to remove. Otherwise, the connector of the memory card slot may be damaged.
- Remove a (dummy) memory card to reposition the device. Moving the device may cause force against the (dummy) memory card, which can damage the connector of the memory card slot.

■ Do not remove the memory card or disconnect power while the ACC LED is lit.

- Lighting of the ACC LED on the front panel indicates that the memory card is being accessed. Never remove the memory card or disconnect power during access. The memory card may be damaged. Some commands require a considerable time before completing access to the memory card after the entry of the commands. Ensure that access is completed and then remove the memory card or disconnect power.

■ Do not attach a label or the like to the transceivers.

- The transceiver has a label indicating its manufacturer and that it is our standard supply. However, this label is attached to the part that does not obstruct heat radiation from the transceiver or the mechanism preventing slip-off from the cage. If a label or the like is attached to such an obstructing part, the transceiver or the network interface module may be damaged.

■ When the ST1 LED is blinking in green, do not power off the device.

- Never disconnect the device power until the ST1 LED on the device front panel changes from blinking in green into being lit. The device may fail.

■ For carrying or packaging the device and optional component, use an antistatic wrist strap.

- Use an antistatic wrist strap. If you handle the device without the antistatic wrist strap, the device can be damaged by the static electricity.

■ When carrying or packing an optional component, take care for handling.

- Take care not to touch the connector when carrying or packing the transceiver, memory card, power supply, fan unit, or power module. They must be stored in antistatic bags when they are not in use.

■ Use air dusters with care.

- Choose an air duster designated to clean optical connectors. Other air dusters may get the end face of the ferrule dirty.
- Avoid the nozzle or container of an air duster from touching the end face of the ferrule. Otherwise, the ferrule may be damaged.

■ Handle the optical connector with care.

- Use the designated optical connector cleaner. Other optical connector cleaners may get the end face of the ferrule dirty.
- Make sure of no problems on the head part of an optical connector cleaner, including attached fabric, grime, and other foreign substances. Otherwise, the end face of the ferrule may be damaged.
- Do not push the optical connector forcibly to clean. Otherwise, the end face of the ferrule may be damaged.
- Rotate an optical connector cleaner (stick type) only in a clockwise direction. An optical connector cleaner rotating clockwise as well as counterclockwise may damage the end face of the ferrule.

■ Maintenance and cleaning

- Wipe off the dirt on the device's outer surface with a dry, clean cloth or a well-wrung wet cloth containing water or neutral cleanser. Do not apply volatile organic solvents or chemicals including benzene and thinner pre-moistened cloths or insect killers, since they can deform, discolor or damage the device.

■ Long-term downtime

- For a long downtime, such as due to a long vacation or travel, be sure to unplug the power cable from the wall outlet for safety. For a configuration using DC power supply, turn off the breaker of the power supply equipment.

■ Discarding the device

- Discard the device according to the ordinance or rule of the local government or call the local waste material handling facility.

1

Overview

This chapter outlines the failure analysis.

[1.1 Failure Analysis Overview](#)

[1.2 System and Partial Failure Analysis Overview](#)

[1.3 Functional Failure Analysis Overview](#)

1.1 Failure Analysis Overview

For any problems with IP8800/S6700, IP8800/S6600, IP8800/S6300, IP8800/S3600, and IP8800/S2400, refer to this manual.

To visually check the system, follow the instructions in "[1.2 System and Partial Failure Analysis Overview](#)."

To login and check the system, follow the instructions in "[1.3 Functional Failure Analysis Overview](#)."

1.2 System and Partial Failure Analysis Overview

1.2.1 Failure Analysis for IP8800/S6700, IP8800/S6600, and IP8800/S6300

If a failure occurs during operation and the system can be visually and directly checked, follow the procedure in "2.1 Troubleshooting for IP8800/S6700, IP8800/S6600, and IP8800/S6300" to troubleshoot.

The device status is displayed on the basic control unit (BCU) for IP8800/S6700, the control and switching unit (CSU) for IP8800/S6600, and management and switching unit (MSU) for IP8800/S6300. LED display of BCS/CSU/MSU is shown in the "Table 1-1: LED Indications, Switches, and Connectors." Also, Front panel layout is shown in the "Figure 1-1: Example of Front Panel Layout."

For LEDs of optional components other than BCU/CSU/MSU shown as an example (BSU, NIF, power supply, and fan unit) and the layout of front panel other than "Figure 1-1: Example of Front Panel Layout," see the manual "Hardware Installation Guide."

Even though the system cannot be visually and directly checked, troubleshooting can be performed similarly by checking system LEDs using the operation command from the remote operation terminal.

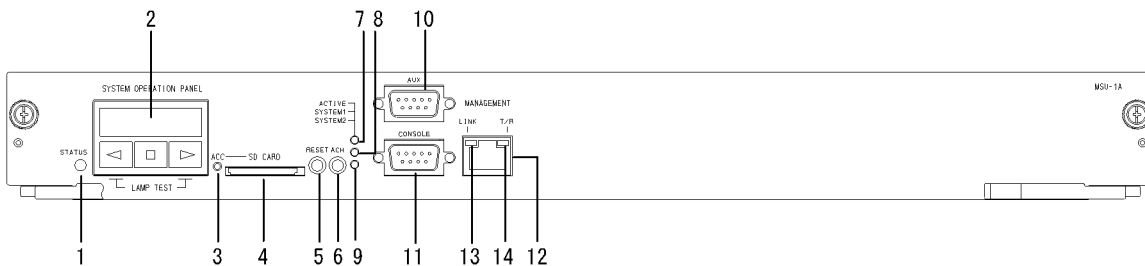
Table 1-1: LED Indications, Switches, and Connectors

No.	Name	Type	Status	Description
1	STATUS	LED: Green/Orange/ Red	Operation status of BCU/ CSU/MSU	Lit in green: Operational Lit in orange: Self-diagnosis in progress Blinking in green: Loading software Lit in red: Failure detected OFF: Power is OFF (BCU/CSU/MSU replaceable)*1
2	SYSTEM OPERATION PANEL	LCD and operation key	System operation panel	Displays the device information, operation instructions, and failure information (for details, see the manual "Configuration Settings")
3	ACC	LED: Green	Memory card status	Lit in green: Accessing the memory card (never detach it). OFF: Memory card in idle state (memory card setting/removal permitted)
4	SD CARD	Connector	SD card slot	SD card slot
5	RESET	Switch (Non-locked)	System manual reset switch	Pressing and holding for a second : When the system fails*2*3 Pressing and holding for 5 seconds : When the password is forgotten*2*4
6	ACH	Switch (Non-locked)	BCU/CSU/MSU switchover switch	When BCU/CSU/MSU is redundant, switchover between the active system and standby system is performed.*2*5
7	ACTIVE	LED: Green	BCU/CSU/MSU operation status	Lit in green: Active system OFF: Standby system
8	SYSTEM1	LED: Green/Orange/ Red	System status	Lit in green: Operational Lit in orange: System partial failure detected Lit in red: System failure detected

No.	Name	Type	Status	Description
9	SYSTEM2	LED: Green/Orange/ Red	Power mode status ^{*6*7}	Lit in green: Power saving mode Blinking in green: Power mode is being changed OFF: Normal power mode Lit in orange: Not supported Lit in red: Not supported
10	AUX	Connector	AUX port	RS-232C port for connecting operation terminal
11	CONSOLE	Connector	CONSOLE port	RS-232C port for connecting operation terminal
12	MANAGEMENT	Connector	MANAGEMENT port	10BASE-T/100BASE-TX Ethernet port for connecting operation terminal
13	LINK	LED: Green/Orange	MANAGEMENT port operation status	Lit in green: Link established Lit in orange: Failure detected OFF: Link failure ^{*8} , or operation shut down ^{*9}
14	T/R	LED: Green	MANAGEMENT port operation status	Lit in green: Sending/receiving packets OFF: Not sending/receiving packets

- *1 BCU/CSU/MSU can be powered off by Inactivate operation from the system operation panel or by inputting the command from the operation terminal.
- *2 The switch is provided in an indented position on the panel surface. Use a thin tip screwdriver to press it.
- *3 If the switch is not pressed and held for at least one second, reset may not occur.
- *4 After the restart, the login password and system administrator password are not required. Therefore, care must be taken to the restart using this method.
- *5 Switchover is only performed when the ACH switch on the active BCU/CSU/MSU is pressed.
- *6 When BSU is used in MSU(IP8800/S6300) and Software Ver11.1 or earlier, lights on the BSU always remain off.
- *7 Only the active system of BSU/CSU indicates power mode status.
- *8 The cable may have slipped off.
- *9 Operation can be shut down by inputting a command.

Figure 1-1: Example of Front Panel Layout



1.2.2 Failure Analysis for IP8800/S3600 and IP8800/S2400

If a failure occurs during operation and the system can be visually and directly checked, follow the procedure in "2.2 Troubleshooting for IP8800/S3600 and IP8800/S2400" to troubleshoot.

For system LEDs of IP8800/S3630-24T2X and IP8800/S2430-24T2X see the figure below and "Table 1-2: LED Indications, Switches, and Connectors."

Even though the system cannot be visually checked, troubleshooting can be performed similarly by checking system LEDs using the operation command from the remote operation terminal.

For IP8800/S3600 and IP8800/S2400, the generic names of the models are as follows:

- AC power supply model: IP8800/S3640-24T, IP8800/S3630-24T, IP8800/S3630-24T2X, IP8800/S3630-24P, IP8800/S2430-24T, IP8800/S2430-24T2X, IP8800/S2430-48T, IP8800/S2430-48T2X
- DC power supply model: IP8800/S3630-24TD, IP8800/S3630-24T2XD, IP8800/S2430-24TD, IP8800/S2430-24T2XD, IP8800/S2430-48TD
- Redundant power supply model: IP8800/S3640-24TW, IP8800/S3640-24T2XW, IP8800/S3640-48TW, IP8800/S3640-48T2XW, IP8800/S3640-24SW, IP8800/S3640-24S2XW, IP8800/S3630-48TW, IP8800/S3630-48T2XW, IP8800/S3630-24S2XW

Figure 1-2: Front Panel Layout

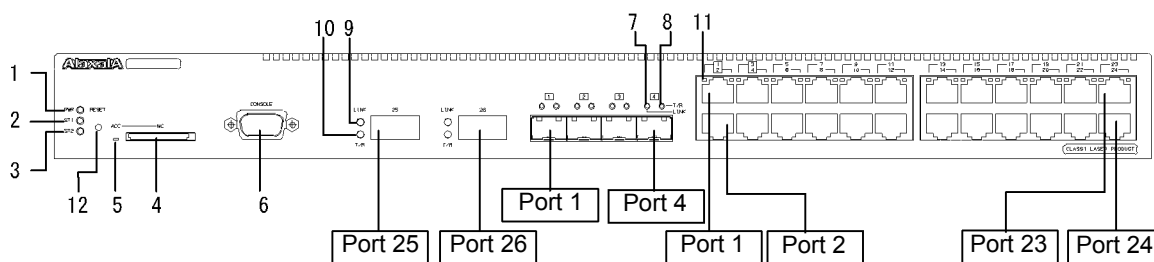


Table 1-2: LED Indications, Switches, and Connectors

No.	Name	Type	Function	Description
1	PWR	LED: Green	Indicates the power ON/OFF status.	Lit in green: Power ON OFF: Power OFF or power failure
2	ST1	LED: Green/Red	Indicates the system status.	Lit in green: Operational Blinking in green: Starting up (starting up) Blinking in red: Partial failure of the device Lit in red: Fatal system failure (operation cannot be continued) OFF: Power OFF or power failure
3	ST2	LED: Green	Always OFF because it is not supported.	
4	MC	Connector	Memory card slot	Memory card slot
5	ACC	LED: Green	Indicates the status of memory card.	ON: Accessing the memory card (the memory card is not detachable) OFF: Memory card is idle (detachable/attachable)
6	CONSOL E	Connector	CONSOLE port	RS-232C port for connecting a console terminal
7	LINK	LED: Green/Orange	Indicates the operation status of Ethernet port in SFP module slot.	Lit in green: Link established Lit in orange: Line failure detected OFF: If ST1 LED is lit in green, the link failed or is blocked.
8	T/R	LED: Green		Lit in green: Sending/receiving frames
9	LINK	LED: Green/Orange	Indicates the operation status of Ethernet port in XFP module slot.	Lit in green: Link established Lit in orange: Line failure detected OFF: If ST1 LED is lit in green, the link failed or is blocked
10	T/R	LED: Green		Blinking in green: Sending/receiving frames

1. Overview

No.	Name	Type	Function	Description
11	1-24	LED: Green/ Orange	Indicates the operation status of 10/ 100/1000BASE-T Ethernet port.	Lit in green: Link established Blinking in green: Link established and frames being sent/received Lit in orange: Line failure detected OFF: If ST1 LED is lit in green, the link failed or is blocked
12	RESET	Switch (Non-locked)	System manual reset switch	Restarts the system.

Note: Figure 1-2 and Table 1-2 show a typical system. For more details on each system, see "Hardware Installation Guide."

1.3 Functional Failure Analysis Overview

The overview of functional failure analysis for this system is shown in the table below.

Some communication failure in the lower layer may cause the communication failure in the upper layer, check the items in the lower layer as well.

Table 1-3: Functional Failure Status and Reference

Item	Subitem	Reference
Forgot login password	Forgot login user password	3.1.1 Forgot the Login User Password
	Forgot system administrator password	3.1.2 Forgot the System Administrator Password
Problems on MC	"MC:-----" is displayed	3.2.1 "MC:-----" is displayed by entering the show system command or the show mc command
	"MC not found." is displayed	3.2.2 "MC not found" is displayed when MC is accessed
Problems on operation terminal	Console input/display disabled	3.3.1 Unable to Input/Display from the Console Correctly
	Remote login disabled	3.3.2 Login from the Remote Operation Terminal Is Failed
	Login authentication disabled	3.3.4 Command Authorization Using RADIUS/TACACS+ Is Disabled
	Command acceptance disabled	3.3.4 Command Authorization Using RADIUS/TACACS+ Is Disabled
Network interface communication failure	Ethernet port communication failure	3.4.1 Ethernet Port Cannot Be Connected
	BSU communication failure [IP8800/S6700]	3.4.2 Communication Failure in Basic Switching Unit BSU/PSP [IP8800/S6700]
	10BASE-T/100BASE-TX/1000BASE-T communication failure	3.4.3 Actions against Troubles on 10BASE-T/100BASE-TX/1000BASE-T
	1000BASE-X communication failure	3.4.4 Actions against Troubles on 1000BASE-X
	10GBASE-R communication failure	3.4.5 Actions against Troubles on 10GBASE-R
	Communication failure while PoE is functioning	3.4.6 Communication Failure on Using PoE
	Link aggregation failure	3.4.7 Communication Failure on Using Link Aggregation
Layer 2 network communication failure	VLAN failure	3.5.1 Layer 2 Communication by VLAN Is Disabled
	Spanning tree failure	3.5.2 Failures on Using Spanning Tree
	Ring Protocol failure	3.5.3 Failures on Using Ring Protocol
	IGMP snooping disabled	3.5.4 Multicast Relay by IGMP snooping Is Disabled
	MLD snooping disabled	3.5.5 Multicast Relay by MLD snooping Is Disabled
IPv4 network communication failure	Communication disabled	3.6.1 Communication Is Disabled or Is Disconnected
	DHCP disabled	3.6.2 IP Addresses Cannot Be Assigned Using DHCP Function
	Dynamic DNS disabled	3.6.3 DynamicDNS Cooperation in DHCP Function Is Disabled

1. Overview

Item	Subitem	Reference
IPv4 unicast routing communication failure	No RIP information	3.7.1 No RIP Routing Information Exists
	No OSPF information	3.7.2 No OSPF Routing Information Exists
	No BGP4 information	3.7.3 No BGP4 Routing Information Exists
	No VRF information	3.7.4 No Routing Information Exist [OP-NPAR]
IPv4 multicast routing communication failure	Communication disabled on PIM-SM network	3.8.1 Communication on IPv4 PIM-SM Network Is Disabled
	Data double-relayed on PIM-SM network	3.8.2 Multicast Data Is Double-relayed on IPv4 PIM-SM Network
	Communication disabled on PIM-SSM network	3.8.3 Communication on IPv4 PIM-SSM Network Is Disabled
	Data double-relayed on PIM-SSM network	3.8.4 Multicast Data Is Double-relayed on IPv4 PIM-SSM Network
	Communication failure of VRF	3.8.5 IPv4 Multicast Communication Failure In VRF [OP-NPAR]
IPv6 network communication failure	Communication disabled	3.9.1 Communication Is Disabled or Is Disconnected
	DHCP trouble	3.9.2 IPv6 DHCP Troubleshooting
IPv6 multicast routing communication failure	No RIPng information	3.10.1 No RIPng Routing Information Exists
	No OSPFv3 information	3.10.2 No OSPFv3 Routing Information Exists
	No BGP4+ information	3.10.3 No BGP4+ Routing Information Exists
IPv6 multicast routing communication failure	Communication disabled on PIM-SM network	3.11.1 Communication on IPv6 PIM-SM Network Is Disabled
	Data double-relayed on PIM-SM network	3.11.2 Multicast Data Is Double-relayed on IPv6 PIM-SM Network
	Communication disabled on PIM-SSM network	3.11.3 Communication on IPv6 PIM-SSM Network Is Disabled
	Data double-relayed on PIM-SSM network	3.11.4 Multicast Data Is Double-relayed on IPv6 PIM-SSM Network
Layer 2 authentication communication failure	Authentication failed in IEEE802.1X	3.12.1 Communication Failure on Using IEEE 802.1X
	Authentication failed in Web authentication	3.12.2 Communication Failure on Using Web Authentication
	Authentication failed in MAC authentication	3.12.3 Communication Failure on Using MAC Authentication
	Authentication failed in authentication VLAN	3.12.4 Communication Failure on Using Authentication VLAN [OP-VAA]
GSRP failure	-	3.13.1 GSRP Communication Failures
IPv4 VRRP failure	-	3.13.2 Communication with VRRP Configuration in IPv4 Network Is Disabled
IPv6 VRRP failure	-	3.13.3 Communication with VRRP Configuration in IPv6 Network Is Disabled
SNMP communication failure	MIB acquisition disabled	3.14.1 MIBs Cannot Be Obtained from SNMP Manager
	Trap receiving disabled	3.14.2 Traps Cannot Be Received by SNMP Manager
sFlow statistics failure	sFlow packet does not reach	3.15.1 sFlow Packets Do Not Reach Collector
	Flow sample does not reach	3.15.2 Flow Sample Does Not Reach Collector
	Counter sample does not reach	3.15.3 Counter Sample Does Not Reach Collector

Item	Subitem	Reference
Neighboring system information cannot be acquired by LLDP function	-	3.16.1 Unable to Obtain Neighboring System Information via LLDP Function
Neighboring system information cannot be acquired by OADP function	-	3.16.2 Unable to Obtain Neighboring System Information via OADP Function
Communication failure in NTP	-	3.17.1 Time Synchronization by NTP Is Disabled
Failure when using IEEE802.3ah/UDLD function	Port becomes inactive	3.18.1 Port Becomes Inactive Due to IEEE802.3ah/UDLD Function
Problems on redundant configuration of basic control unit (BCU)/control and switching unit (CSU)/management and switching unit (MSU) [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]	-	3.19.1 Active System Switchover Is Disabled
Problems on redundant configuration of basic switching unit (BSU) [IP8800/S6700]	BSU switchover disabled	3.20.1 Active BSU Switchover Is Disabled
Problem on using power saving function	Schedule is disabled [IP8800/S6700] [IP8800/S6600]	3.21.1 Schedule Is Disabled [IP8800/S6700] [IP8800/S6600]
Communication failure due to discard of packets	-	3.23.1 Checking Filtering/QoS Setting Information
Communication failure due to resource shortage [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]	The volume of MAC address table used exceeds the accommodating condition.	4.1 MAC Address Table Resource Shortage
	The volume of VLAN identification table used exceeds the accommodating condition.	4.2 When Resource Shortage of VLAN Identification Table Occurs
	Resource shortage of shared memory	4.3 When Resource Shortage Occurs in Shared Memory
Others	-	Re-check the setting according to "Configuration Settings."

2

Troubleshooting System Failures

This chapter explains how to deal with the problems on the system.

[2.1 Troubleshooting for IP8800/S6700, IP8800/S6600, and IP8800/S6300](#)

[2.2 Troubleshooting for IP8800/S3600 and IP8800/S2400](#)

2.1 Troubleshooting for IP8800/S6700, IP8800/S6600, and IP8800/S6300

2.1.1 Troubleshooting Procedure on System Failures

Follow the procedure below when the system failed.

Table 2-1: Troubleshooting System Failures

No.	Failure	Action
1	<ul style="list-style-type: none"> • Fume generated from the system • Unusual odor occurs from the system • Unusual sound occurs from the system 	<p>Execute the steps below immediately.</p> <ol style="list-style-type: none"> 1. Power off the system. 2. When the power cable is fastened by the slip-off preventive clamp, remove it from the power cable. 3. For AC power supply, unplug the power cable. 4. For DC power supply, turn off the breaker of power distribution panel connected to the system. <p>Shut down operation as described above and then contact the local sales office.</p>
2	login prompt is not displayed	<ol style="list-style-type: none"> 1. When MC is inserted, first remove the MC then reboot the system by turning it off and on. 2. When MC is not inserted, reboot the system by turning it off and on. 3. If the same problem still persists after system reboot, replace BCU/CSU/MSU.
3	All LEDs on BCU/MSU are OFF	<ol style="list-style-type: none"> 1. Check LED on the power supply and follow the steps below. <ol style="list-style-type: none"> (1) If ALARM LED is lit in red on the power supply, replace the power supply with a new one. (2) If both POWER LED and ALARM LED are OFF on the power supply, implement "Table 2-2: Power Failure Check Items." If the problem is not settled, replace the power supply with LED turned off. 2. If all power supplies are running normally, replace BCU/CSU/MSU.
4	BCU/CSU/MSU SYSTEM1 LED lit in red or orange	<ol style="list-style-type: none"> 1. If an error message is output to the system operation panel, take the action against the corresponding error message in manual "Message Log Reference." 2. If no error message is output, replace BCU, BSU, CSU, MSU or NIF on which STATUS LED is lit in red.

No.	Failure	Action
5	Error message output to the system operation panel	Take the action against the corresponding error message in the manual "Message Log Reference."
6	STATUS LED on BCU/CSU/MSU is lit in red, other LEDs are OFF, and no message on the system operation panel	<ol style="list-style-type: none"> Check the single/redundant configuration of BCU/CSU/MSU. <ol style="list-style-type: none"> For the single configuration, follow the step 3 and later. For the redundant configuration, follow the step 2 and later. Check the active/standby state of BCU/CSU/MSU. <ol style="list-style-type: none"> If the failure occurs only in one system, replace the BCU/CSU/MSU. You do not have to follow the step 3 and later. If the failure occurs in both systems, follow the step 3 and later. Check the LED on the power supply. <ol style="list-style-type: none"> If ALARM LED is lit in red on the power supply, replace the power supply with a new one. If both POWER LED and ALARM LED are OFF on the power supply, implement "Table 2-2: Power Failure Check Items" If the problem is not settled, replace the power supply with LED turned off. If all power supplies are running normally, leave those power supplies as is. Turn off all power supplies installed on the system. At least two seconds elapse, turn on all power supplies installed on the system. <ol style="list-style-type: none"> If this failure occurs on BCU/CSU/MSU, replace the BCU/CSU/MSU.

Table 2-2: Power Failure Check Items

No.	Failure	Action
1	Power switch on the power supply is OFF	Turn on the power switch.
2	<ul style="list-style-type: none"> Power cable is unplugged Power cable is not firmly connected to the system Power cable is not securely fastened by the slip-off preventive clamp 	<p>Follow the steps below.</p> <ol style="list-style-type: none"> Turn off the power switch. For DC power supply, turn off the breaker of power distribution panel connected to the system. Connect the power cable correctly. If the power cable can be fastened by the slip-off preventive clamp, fasten the power cable using it. For DC power supply, turn on the breaker of power distribution panel connected to the system. Turn on the power switch.
3	Power supply is not securely mounted but loose	<p>Follow the steps below.</p> <ol style="list-style-type: none"> Turn off the power switch. For DC power supply, turn off the breaker of power distribution panel connected to the system. When the power cable is fastened by the slip-off preventive clamp, remove it from the power cable. Remove the power cable. Remove the power supply and insert it securely. Attach the power cable. If the power cable can be fastened by the slip-off preventive clamp, fasten the power cable using it. For DC power supply, turn on the breaker of power distribution panel connected to the system. Turn on the power switch.
4	<p>Measured input power is out of the range below.</p> <p>100VAC: 90 to 132VAC 200VAC: 180 to 264VAC -48VDC: -40.5 to -57VDC</p> <p>Note: Implement this matter only if input power can be measured.</p>	Contact the person in charge of the power facility and ask him/her to take the action for input power.

2.1.2 Replacement Method of Optional Components

The optional component replacement procedures are described in "Hardware Installation Guide." Follow the procedures described in the manual.

2.2 Troubleshooting for IP8800/S3600 and IP8800/S2400

2.2.1 Troubleshooting Procedure on System Failures

Follow the procedure below when the system failed.

Table 2-3: Troubleshooting System Failures

No.	Failure	Action
1	<ul style="list-style-type: none"> • Fume generated from the system • Unusual odor occurs from the system • Unusual sound occurs from the system 	Execute the steps below immediately. <ol style="list-style-type: none"> 1. Power off the system. 2. Remove the power cable of the system. After the above steps, replace the system.
2	login prompt is not displayed	<ol style="list-style-type: none"> 1. When MC is inserted, first remove the MC then reboot the system by turning it off and on. 2. When MC is not inserted, reboot the system by turning it off and on. 3. If the same problem still persists after system reboot, replace the system.
3	PWR LED on the system is OFF	Follow the steps below to take the action. <ol style="list-style-type: none"> 1. Follow the steps in "Table 2-4: Isolating Power Supply Failure" 2. For the redundant power model, replace the power supply that has failed. The faulty power supply is in one of the states below. <ol style="list-style-type: none"> (a) POWER LED is off. (b) ALM1 LED is lit in red. (c) ALM2 LED is lit in red. 3. If 1 and 2 are not applicable, restart the system and confirm that the environment is free from troubles. <ol style="list-style-type: none"> (1) Turn off the power switch on the system (or power supply for the redundant power model) and turn it on again to restart the system. (2) If the system can be restarted, execute the <code>show logging</code> command to view the failure information. <pre>>show logging grep ERR</pre> (3) If a message "Caution, High temperature" exists in the retrieved failure information, the operating environment may have caused the failure. Request the system administrator to improve the environment. (4) If the system cannot be restarted by procedure (1) above and no failure information exists in procedure (3) above or message "Caution, High temperature" does not exist, the system may have failed. Replace the system.
4	ST1 LED on the system is lit in red	A failure occurred or the system was powered on after it had remained powered off for a long time (at least one month). <ol style="list-style-type: none"> 1. If you do not turn on the power of the system for a long time (one month or more), reboot the system by turning it off and on. 2. In the case of other than the previous case, a failure might occur in the system. Replace the system.

2. Troubleshooting System Failures

No.	Failure	Action
5	<ul style="list-style-type: none"> ST1 LED on the system is blinking in red LINK LED (10GBASE-R port and 1000BASE-X port) and 1-48 LED (10/100/1000BASE-T port) on each port of the system are lit in orange or OFF 	<p>System or line has failed.</p> <ol style="list-style-type: none"> For the redundant power supply model, check the states of the power supplies and fan unit. Replace them if they have failed. <ul style="list-style-type: none"> If ALM LED on the fan unit is lit in red, replace the fan unit. If ALM1 LED or ALM2 LED or the power supply is lit in red, replace the power supply. If POWER LED on the power supply is off, take the action against power failure according to "Table 2-4: Isolating Power Supply Failure." If POWER LED is still off after the action is taken, replace the power supply. For cases other than 1 above, refer to the error message and take the action against the failure. Execute the <code>show logging</code> command to check the failure information and take the action. <pre>>show logging grep ERR</pre> For the failure on the external power unit, refer to "2.2.2 Isolating Failures on External Power Unit" to isolate the failure.
6	"EPU:Disconnect" is displayed for the system management command although LEDs on the system and external power unit are normal	<p>Check the cable interconnecting the system and EPU. If the cable has slipped off, restart the system as described below.</p> <ol style="list-style-type: none"> Power off the system. Reconnect the cable that has slipped off. Power off the system.

Table 2-4: Isolating Power Supply Failure

No.	Failure	Action
1	Power switch on the system (or power supply for the redundant power model) is OFF	Turn on the power switch.
2	Power cable has slipped off or is loose	<p>Follow the steps below.</p> <ol style="list-style-type: none"> Turn off the power switch. Connect the power cable correctly. Turn on the power switch.
3	For the redundant power supply model, the power supply is not securely mounted but loose	<p>Follow the steps below.</p> <ol style="list-style-type: none"> Turn off the power switch. Insert the power supply correctly. Turn on the power switch.
4	<p>Measured input power is out of the range below.</p> <p>100VAC: 90 to 127VAC 200VAC: 180 to 254VAC -48VDC: -40.5 to -57VDC</p> <p>Note: Implement this matter only if input power can be measured.</p>	Contact the person in charge of the power facility and ask him/her to take the action for input power.

2.2.2 Isolating Failures on External Power Unit

If the external power unit fails, follow the steps below to isolate the failure.

Table 2-5: Isolating Failures on External Power Unit

No.	Failure	Action
1	POWER LED on the external power unit is lit in green	<p>Check LED on the power module mounted on the external power unit and identify the power module that is not normally running. If the power module is normally running, the states below are provided.</p> <ul style="list-style-type: none"> • EPU-A: DC-OK: Lit in green, DC-ALM: OFF • EPU-B: DC-OK: Lit in green, DC-FAIL: OFF, AC-OK: Lit in green <p>For the power module that is not normally running, implement "Table 2-7: Isolating Failures on Power Module."</p>
2	POWER LED on the external power unit is OFF	Follow the steps in " Table 2-6: Isolating Failures on External Power Unit (Main Body) ."

Table 2-6: Isolating Failures on External Power Unit (Main Body)

No.	Failure	Action
1	Power switch on the external power unit is OFF	Turn on the power switch.
2	Power cable of the external power unit is not correctly connected to the system	<ol style="list-style-type: none"> 1. Turn off the power switch. 2. Connect the power cable correctly. 3. Turn on the power switch.
3	Input power to the external power unit is out of the range below (AC power supply: 90 to 132V)	Ask the system administrator to take the action because of the failure on the power supply facility (i.e. not the failure on this system).
4	Other than 1 to 3 above	Replace the external power unit.

Table 2-7: Isolating Failures on Power Module

No.	Failure	Action
1	Power switch on the power module is OFF	Turn on the power switch on the power module.
2	Power cable of the power module is not correctly connected to the system	<ol style="list-style-type: none"> 1. Turn off the power switch on the power module. 2. Connect the power cable correctly. 3. Turn on the power switch on the power module.
3	Power module is not correctly mounted on the external power unit	<ol style="list-style-type: none"> 1. Turn off the power switch. 2. Mount the power module correctly. 3. Turn on the power switch.
4	Other than 1 to 3 above	Replace the power module.

2.2.3 Replacement Method of System and Optional Components

The replacement procedures for optional components are described in "Hardware Installation Guide." Follow the procedures described in the manual.

3

Troubleshooting Functional Failures in Operation

This chapter describes actions to be taken when the system does not operate normally or the communication is not possible.

[3.1 Problems on Login Password](#)

[3.2 Problems on MC](#)

[3.3 Problems on Operation Terminal](#)

[3.4 Network Interface Communication Failure](#)

[3.5 Layer 2 Network Communication Failure](#)

[3.6 IPv4 Network Communication Failure](#)

[3.7 IPv4 Unicast Routing Communication Failure](#)

[3.8 IPv4 Multicast Routing Communication Failure](#)

[3.9 IPv6 Network Communication Failure](#)

[3.10 IPv6 Unicast Routing Communication Failure](#)

[3.11 IPv6 Multicast Routing Communication Failure](#)

[3.12 Layer 2 Authentication Communication Failure](#)

[3.13 Communication Failure on High-reliability Function](#)

[3.14 SNMP Communication Failure](#)

[3.15 Troubleshooting of sFlow Statistics \(Flow Statistics\) Function](#)

[3.16 Communication Failures on Neighboring System Managing Function](#)

[3.17 NTP Communication Failure](#)

[3.18 Communication Failure on IEEE802.3ah/UDLD Function](#)

[3.19 Problems on Redundant Configuration of Basic Control Unit \(BCU\)/Control and Switching Unit \(CSU\)/Management and Switching Unit \(MSU\) \[IP8800/S6700\] \[IP8800/S6600\] \[IP8800/S6300\]](#)

3. Troubleshooting Functional Failures in Operation

[3.20 Problems on Redundant Configuration of Basic Switching Unit \(BSU\) \[IP8800/S6700\]](#)

[3.23 Communication Failure Caused by Settings of Filtering/QoS](#)

3.1 Problems on Login Password

3.1.1 Forgot the Login User Password

If you forgot the login user password and cannot login to the system during operation, follow the procedure below.

1. Reporting to the system administrator

First, consult the system administrator. However, if there is no login user eligible for the administrator (e.g., there is no other login user), perform a default restart and set a password again.

Default restart

Press and hold the reset switch on the system for five or more seconds.

Since security check using a password is not performed, special care must be taken when doing default restart.

The password setting is enabled after starting the system.

2. Changing the password

When a password change is requested, the system administrator must change it and inform all the target login users of the change (use the `password` command to change a password, or the `clear password` command to simply delete it).

Figure 3-1: Changing Login User Password by System Administrator

```
# password user1
Changing local password for user1.
New password:
Retype new password:
#
```

3.1.2 Forgot the System Administrator Password

If all the login users with the system administrator privilege forgot the system administrator password and they cannot enter the system administrator mode, perform the default restart to set up a password again.

Default restart

Press and hold the reset switch on the system for five or more seconds.

Since security check using a password is not performed, special care must be taken when doing default restart. The password setting is valid after restarting the system.

3.2 Problems on MC

3.2.1 "MC:-----" is displayed by entering the show system command or the show mc command

When "MC:-----" is displayed by entering the `show system` command or the `show mc` command, follow the instruction in "[Table 3-1: Problems and Actions When "MC:-----" is displayed](#)"

Table 3-1: Problems and Actions When "MC:-----" is displayed

No.	Failure	Troubleshooting Steps
1	Check to see ACC LED.	When ACC LED is lit in green, it indicates other process might be accessing to MC. After the ACC LED lights off, execute the command again. If the ACC LED is not lit in green, follow the instructions on No.2 and later.
2	Remove the MC then insert it.	After removing and inserting MC, execute the command again. Confirm that no dust is attached on the MC or the memory card. If dust is adhere to them, clean it with a dry cloth then insert the MC. If a symptom still occurs after you have removed and inserted the MC for several times, follow the instructions on No.3.
3	Replace the MC with a new one.	Replace the MC then execute the command again. If a fault still occurs after the MC has been replaced, memory slot card might be broken. In this case, replace the BCU [IP8800/S6700] , the CSU [IP8800/S6600] , the MSU [IP8800/S6300] , the system [IP8800/S3600] , or the system [IP8800/S2400] .

3.2.2 "MC not found" is displayed when MC is accessed

When "MC not found" is displayed after the command for accessing to MC has been executed, follow the instruction in "[Table 3-2: Problems and Actions When "MC not found" is displayed.](#)"

Table 3-2: Problems and Actions When "MC not found" is displayed

No.	Failure	Troubleshooting Steps
1	Check to see ACC LED.	When ACC LED is lit in green, it indicates other process might be accessing to MC. After the ACC LED lights off, execute the command again. If ACC LED is not lit in green, follow the instructions on No.2 and later.
2	Remove the MC then insert it.	After removing and inserting MC, execute the command again. Check to see that any dust is not attached on the MC or the memory card. If dust is adhere to them, clean it with a dry cloth then insert the MC. If a symptom still occurs after you have removed and inserted the MC for several times, follow the instructions on No.3.
3	Replace the MC with a new one.	Replace the MC then execute the command again. If a fault still occurs after the MC has been replaced, memory slot card might be broken. In this case, replace the BCU [IP8800/S6700] , the CSU [IP8800/S6600] , the MSU [IP8800/S6300] , or the system [IP8800/S3600] [IP8800/S2400] .

3.3 Problems on Operation Terminal

3.3.1 Unable to Input/Display from the Console Correctly

When there is a problem connecting to the console, follow the instruction in "[Table 3-3: Problems and Actions When Connecting to Console.](#)"

When there is a problem connecting to the modem, follow the instruction in "[Table 3-4: Problems and Actions When Connecting to Modem.](#)" Also, see the manual provided with the modem.

Table 3-3: Problems and Actions When Connecting to Console

No.	Failure	Troubleshooting Steps
1	Nothing is displayed on the screen.	Determine the cause by following the steps below: <ol style="list-style-type: none"> 1. Check if the ST1 LED on the front panel of the system lights in green. If it is not, see "1.2 System and Partial Failure Analysis Overview." 2. Check to see if the cable is connected correctly. 3. Confirm that RS232C cross cable is used. 4. Confirm that communication software settings, including port number, communication rate, data length, parity bit, stop bit, flow control are set as follows: Communication rate: 9600 bps (or a custom value) Data length: 8 bits Parity bit: None Stop bit: 1 bit Flow control: None
2	You cannot enter any key.	Determine the cause by following the steps below: <ol style="list-style-type: none"> 1. Data sending/receiving may be interrupted by the XON/XOFF flow control. Restart the data sending/receiving (press [Q] key with the [Ctrl] key pressed). If the problem continues, follow the instructions on No.2 and later. 2. Check to see if the communication software is configured properly. 3. The screen may be suspended by [Ctrl]+[S]. Press any key.
3	Abnormal characters are displayed upon login.	Negotiation with the communication software may have failed. Check the communication rate of the communication software as described below. <ol style="list-style-type: none"> 1. If the communication rate for the CONSOLE (RS232C) has not been set up using configuration command <code>line console 0</code>, check to see if the communication rate is set to 9600 bps in the communication software. 2. If the communication rate for the CONSOLE (RS232C) is set to 1200, 2400, 4800, 9600 or 19200 bps using configuration command <code>line console 0</code>, confirm that the communication rate in the communication software has been correctly set.
4	Abnormal characters appears while entering user name.	Communication rate for the CONSOLE (RS232C) may have been changed. See No. 3.
5	Login is disabled.	Confirm that the login prompt appears on the screen. If it is not the case, starting up the system is on the way. Wait for a while.
6	Abnormal characters appear and command entry is rejected when the communication rate of the communication software is changed after login.	If the communication rate of the communication software is changed after login, normal display is not achieved. Reset the communication rate of the communication software to the original setting.
7	Abnormal characters appear upon login with HyperTerminal.	Negotiation with the communication software may have failed. See No. 3. Issue a break signal using [Alt]+[B]. Depending on the communication rate in HyperTerminal, login screen may not appear until you issue several break signals.
8	Item names and contents are not displayed in line.	The size of information might be too large to display within one line. Change the screen size by setting the communication software and increase the number of characters that can be displayed in one line.

Table 3-4: Problems and Actions When Connecting to Modem

No.	Failure	Troubleshooting Steps
1	Automatic termination to the modem is disabled.	Check the following. <ul style="list-style-type: none"> • Cable is connected properly. • Modem is powered on. • Telephone number is correct. • Settings of the modem are correct. • Line can be connected by connecting the modem to two terminals and dialing.
2	Abnormal characters are displayed upon login.	Determine the cause by following the steps below: <ol style="list-style-type: none"> 1. Set the baud rate of the modem to 9600 bps. 2. If the modem supports communication standard V90, K56flex, x2, or later, set the modem so that it is connected via V.34 communication method or below.
3	Line is busy and cannot be connected by redialing after disconnection.	Termination may be disabled for several seconds after disconnection of the line. See the manual provided with the modem.
4	Line cannot be reconnected after line failure.	When the line is disconnected due to a failure, reconnection may be disabled for up to 120 seconds. If you want to connect the line immediately, login via another method, and use the <code>killuser</code> command to apply forced logout to the user who connected AUX by dial-up IP connection.
5	Line cannot be reconnected after disconnection.	When dial-up IP connection is disconnected, it might take time to reconnect the line. In this case, wait for approximately 30 seconds then reconnect the line.

3.3.2 Login from the Remote Operation Terminal Is Failed

When connecting to the remote operation terminal fails, take actions in the following table.

Table 3-5: Problems and Actions When Connecting Remote Operation Terminal

No.	Symptom	Action to Be Taken or Reference
1	Remote connection rejected.	Determine the cause by following the steps below: <ol style="list-style-type: none"> 1. To make sure the route for the remote connection has been established, execute the <code>ping</code> command from a PC or workstation. 2. After the message indicating the connection has been established is displayed, if it needs much time to display the prompt, communication with the DNS server may possibly be disabled. (If this is the case, it takes approximately five minutes until the prompt is displayed, which is a typical value and usually depends on network conditions.)
2	Login rejected.	Determine the cause by following the steps below: <ol style="list-style-type: none"> 1. Check to see if the terminal used has the IP or IPv6 address allowed by the access list for the configuration command <code>line vty</code> mode. Furthermore, confirm that <code>deny</code> has not been set for the IP or IPv6 address on the access list in the configuration command (for details, see the manual "Configuration Commands, Vol. 1"). 2. Confirm that maximum number of login users has not been exceeded (for details, see the manual "Configuration Settings"). If reachability from the remote operation terminal to this system is lost when the maximum number of users have logged in and then the reachability is recovered, a remote operation terminal cannot log in to the system until the time of TCP protocol timeout elapses to clear the session. The time of TCP protocol timeout is approximately 10 minutes although it depends on the states of the remote operation terminal and network. 3. Check to see if protocols restricted by the configuration command <code>transport input</code> in <code>line vty</code> mode are not being used. For more details, see the manual "Configuration Commands."

No.	Symptom	Action to Be Taken or Reference
3	Key entry rejected.	Determine the cause by following the steps below: 1. Data sending/receiving may be interrupted by the XON/XOFF flow control. Restart the data sending/receiving (press [Q] key with the [Ctrl] key pressed). If key entry is still disabled, check No. 2 or later. 2. Check to see if the communication software is configured properly. 3. The screen may be suspended by [Ctrl]+[S]. Press any key.
4	Some users remain in the login state.	Wait for automatic logout or log in again and use the <code>killuser</code> command to delete users in the login state. If editing the configuration is on the way, the possibly changed configuration information has not been saved. Log in again and enter the configuration mode to save the change and exit from the editing.

3.3.3 Login Authentication Using RADIUS/TACACS+ Is Disabled

If login authentication using RADIUS/TACACS+ is failed, check the following:

1. Communication with the RADIUS/TACACS+ server
 Use the `ping` command to see if communication from this system to the RADIUS/TACACS+ server is achieved. If it is not possible to communicate with the server, see "[3.6.1 Communication Is Disabled or Is Disconnected.](#)" If a local address has been defined in configuration, check the connectivity between this system and RADIUS/ TACACS+ servers by issuing `ping` from the local address.
2. Setting timeout value and retry count
 For the RADIUS authentication, you can use configuration commands `radius-server host`, `radius-server retransmit`, and `radius-server timeout` to determine the maximum value of the timeout, which determines that communication between this system and the RADIUS server is faulty. This value is calculated by `<set timeout value (sec.)> × <set retry count> × <set number of RADIUS servers>`.
 For the TACACS+ authentication, you can use configuration commands `tacacs-server host` and `tacacs-server timeout` to determine the maximum value of the timeout, which determines that communication between this system and TACACS+ server is faulty. This value is calculated by `<set timeout value (sec.)> × <set number of TACACS+ servers>`. If this time is extremely long, applications such as telnet on the remote operation terminal may be terminated as a result of timeout. If this is the case, edit the value on the RADIUS/ TACACS+ configuration or the timeout value on the application running on the remote operation terminal. If telnet or ftp fails despite the "RADIUS/TACACS+ authentication successful" message appears in the operation log, the application on the remote operation terminal may have timed out until it can connect to the running RADIUS/ TACACS+ server out of multiple RADIUS server specified in the configuration. In this case, make sure you set up that the running RADIUS/TACACS+ server will take precedence or decrease the `<Timeout value (in seconds)> × <Number of retries>` value.

3.3.4 Command Authorization Using RADIUS/TACACS+ Is Disabled

If command authorization fails even when login to this system through RADIUS/TACACS+ authentication was successful, or if an authorization error message is displayed and command cannot be executed, check the following:

1. Check using the `show whoami` command
 Using the `show whoami` command on this system, the list of operation commands permitted/limited for the current user can be displayed and checked. Confirm that the command list has been acquired according to the setting on the RADIUS or TACACS+ server.
2. Check for server settings
 Confirm that setting on command authorization on this system is correct on the RADIUS/TACACS+ server. For RADIUS, beware the settings for vendor-specific attributes. For TACACS+, beware service and attribute name. For detail on the RADIUS/TACACS+ server settings, see the manual "Configuration Settings."

3. Troubleshooting Functional Failures in Operation

3. Notes on writing command list

Care must be taken about the handling of spaces when you describe the command list for the command authorization on this system on the RADIUS/TACACS+ server. For example, if `show ip` (`show ip` followed by a space) is set in the permitted command list, the `show ip interface` command is permitted but the `show ipv6 interface` command is prohibited.

3.4 Network Interface Communication Failure

3.4.1 Ethernet Port Cannot Be Connected

If the Ethernet port has possibly caused the communication failure, check for the NIF **[IP8800/S6700]** **[IP8800/S6600]** **[IP8800/S6300]** and port statuses as follows.

(1) Checking NIF status **[IP8800/S6700]** **[IP8800/S6600]** **[IP8800/S6300]**

1. Checking log

For the log, see the manual "Message Log Reference."

2. Isolating the problem according to the NIF status.

Check the NIF status by using the `show interfaces` command, and isolate the problem according to the table below.

Table 3-6: Check and Action for NIF Status

No.	NIF Status	Problem	Action
1	active	The NIF is operating normally.	Check the port status according to "Table 3-7: Check and Action for Port Status."
2	notconnect	The NIF is not installed.	Install the NIF board.
3	inactive	The <code>inactivate</code> command is set.	Use the <code>activate</code> command to activate the NIF.
		The NIF is not fully inserted.	Install the NIF board correctly.
		NIF is not activated.	Use the <code>show system</code> command to check the BSU operation status and set the operation status to "active." [IP8800/S6700]
			Use the <code>show system</code> command to check the PSP operation status and set the operation status to "active." [IP8800/S6600] [IP8800/S6300]
		NIF not supported by the software version is installed.	Check the NIF board type and software version. Replace the NIF board or update the software.
NIF not supported by this system is installed.	Replace the NIF board.		
4	fault	The NIF is faulty.	According to the log of the NIF displayed by the <code>show logging</code> command, see the corresponding part in the manual "Message Log Reference" and follow the descriptions in [Action].
5	initialize	The NIF is being initialized.	Wait until initialization completes.
6	disable	<code>no power enable</code> is set by configuration command.	Confirm that the NIF board to be used is installed and enter configuration command <code>power enable</code> to activate the NIF.

(2) Checking port status

1. Checking log

For the log, see the manual "Message Log Reference."

2. Isolating the problem according to the port status.

Check the port status by using the `show interfaces` command, and isolate the problem according to the table below.

3. Troubleshooting Functional Failures in Operation

Table 3-7: Check and Action for Port Status

No.	Port Status	Problem	Action
1	active up	The port is operating normally.	None
2	active down	Line failure occurred in the port.	According to the log of the port displayed by the <code>show logging</code> command, see the corresponding part in manual "Message Log Reference" and follow [Action] described.
3	inactive	<p>The inactive state is set by one of the following:</p> <ul style="list-style-type: none"> • The <code>inactivate</code> command • Standby link of link aggregation • BPDU guard function of a spanning tree • GSRP port-reset function • Failure detected by the IEEE802.3ah/UDLD function • Port blocked by L2 loop detection function • Port blocked by the storm control function 	<ul style="list-style-type: none"> • If the inactive state is set by standby link function of link aggregation, it is a normal operation and therefore do not set the active state using the <code>activate</code> command. Check standby link function using the <code>show channel-group</code> command with "detail" parameter specified. • If the inactive state is set by the BPDU guard function of a spanning tree, review the configuration of the opposite system. Set up the configuration so that this system will not receive BPDU. Using the <code>activate</code> command, set the port to the active state. Check BPDU guard function using the <code>show spanning-tree</code> command with "detail" parameter specified. • If the inactive state is set by the port reset function of GSRP, the active state automatically restores. Since this is a normal operation, do not set to the active state using the <code>activate</code> command. • If the inactive state is set by detection of one-way link failure or L2 loop by IEEE802.3ah/UDLD function, see "3.18 Communication Failure on IEEE802.3ah/UDLD Function." After recovery from failure, use the <code>activate</code> command to activate the port. • When ports blocked by L2 loop detection function are in inactive status, change the configuration, which causes the loop. And then enable the inactive port by using the <code>activate</code> command. At this time, if <code>loop-detection auto-restore-time</code> has been set by the configuration command, the ports will change status to active status automatically. • If the inactive state is set by the storm control function, use the <code>activate</code> command to activate the port after LAN recovered from the storm. • If you want to set the active in any other case, confirm that the cable is connected to the port to be used and use the <code>activate</code> command to activate the port.
4	test	The port is in the line test by the <code>test interfaces</code> command.	To restart communication, execute the <code>no test interfaces</code> command to stop the line test and activate the port with the <code>activate</code> command.
5	fault	Hardware of the port is faulty.	According to the log of the port displayed by the <code>show logging</code> command, see the corresponding part in manual "Message Log Reference" and follow [Action] described.
6	initialize	The port is being initialized.	Wait until initialization completes.
7	disable or locked	Configuration command <code>shutdown</code> is set.	Confirm that the cable is connected to the port to be used and enter configuration command <code>no shutdown</code> to activate the port.

(3) Checking statistical information

Enter the `show port statistics` command to check the number of sent/received packets and the number of discarded packets on all ports installed on this system.

Figure 3-2: Example of "Checking Port Operation Status" [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]

```

> show port statistics
2006/03/23 12:00:00
Port Counts:48
Port Name Status T/R Unicast Multicast Broadcast Discard
1/ 1 geth1/1 up Tx 0 0 0 0
Rx 0 0 0 0
1/ 2 geth1/2 down Tx 0 0 0 0
Rx 0 0 0 0
1/ 3 geth1/3 down Tx 0 0 0 0
Rx 0 0 0 0
(Omitted hereafter)
>

```

Figure 3-3: Example of "Checking Port Operation Status" [IP8800/S3600] [IP8800/S2400]

```

> show port statistics
2006/03/23 12:00:00
Port Counts:48
Port Name Status T/R All packets Multicast Broadcast Discard
0/ 1 geth0/1 up Tx 0 0 0 0
Rx 0 0 0 0
0/ 2 geth0/2 down Tx 0 0 0 0
Rx 0 0 0 0
0/ 3 geth0/3 down Tx 0 0 0 0
Rx 0 0 0 0
(Omitted hereafter)
>

```

If display item "Discard" is larger than 0 when this command is executed, a failure discarding packets has occurred. Use the `show interfaces` command to retrieve detail information of the port.

3.4.2 Communication Failure in Basic Switching Unit BSU/PSP

If BSU/PSP has possibly caused the communication failure, check for the BSU/PSP status as follows.

(1) Checking BSU/PSP operation status

1. Checking log

For the log, see the manual "Message Log Reference."

2. Isolating the problem according to the BSU/PSP operation status

Check the BSU/PSP operation status by using the `show system` command, and isolate the problem according to the table below.

Table 3-8: Check and Action for BSU/PSP Operation Status

No.	BSU Operation Status	Problem	Action
1	active	The BSU/PSP is operating as active system.	See " 3.4.1 Ethernet Port Cannot Be Connected. "
2	standby hot	The BSU/PSP is operating as standby system in hot standby mode.	See " 3.4.1 Ethernet Port Cannot Be Connected. "
3	standby cold [IP8800/S6700]	The BSU/PSP is operating as standby system in cold standby mode.	See " 3.4.1 Ethernet Port Cannot Be Connected. "
4	standby cold2 [IP8800/S6700] [IP8800/S6600]	The BSU/PSP is operating as standby system in cold standby 2 mode.	See " 3.4.1 Ethernet Port Cannot Be Connected. "

3. Troubleshooting Functional Failures in Operation

No.	BSU Operation Status	Problem	Action
5	fault	Unavailable configuration has been set.	Use configuration command <code>fldm prefer</code> to correctly set flow distribution pattern of the filter and QoS function.
6			Use configuration command <code>fwdm prefer</code> to correctly set the distribution pattern of the maximum number of entries per device.
7		The BSU/PSP is faulty.	According to the log of the BSU displayed by the <code>show logging</code> command, see the corresponding part in manual "Message Log Reference" and follow [Action] described.
8	inactive [IP8800/S6700]	The <code>inactivate bsu</code> command is set.	Use the <code>activate bsu</code> command to make the BSU active, standby hot, or standby cold status. If it does not become standby hot or standby cold status, see " 3.20 Problems on Redundant Configuration of Basic Switching Unit (BSU) [IP8800/S6700] ."
9		The BSU is not fully inserted.	Install the BSU board correctly.
10		Different type of BSUs are installed together.	Unify the type of all BSU boards.
11		BSU not supported by the software version is installed.	Check the BSU board type and software version. Replace the BSU board or update the software.
12		BSU not supported by this device is installed.	Replace the BSU board.
13	notconnect [IP8800/S6700]	The BSU is not installed.	Check if as many BSU boards as required for active BSU + standby BSU (if standby BSU is not required, only active BSU) are installed. If so, no action is required. If not so, install the required number of BSU boards.
14	initialize	The BSU/PSP is being initialized.	Wait until initialization completes.
15	disable [IP8800/S6700]	<code>no power enable</code> is set by configuration command.	After checking that the BSU board to be used is installed, use configuration command <code>power enable</code> to make the BSU active, standby hot, or standby cold status. If it does not become standby hot or standby cold status, see " 3.20 Problems on Redundant Configuration of Basic Switching Unit (BSU) [IP8800/S6700] ."

3.4.3 Actions against Troubles on 10BASE-T/100BASE-TX/1000BASE-T

If a trouble occurs on 10BASE-T/100BASE-TX/1000BASE-T, follow the procedure below to isolate the problem.

1. Checking log
For the log, see the manual "Message Log Reference."
2. Isolating the problem according to the failure analysis method
Isolate the problem according to the failure analysis method listed below.

Table 3-9: Troubleshooting for Failed 10BASE-T/100BASE-TX/1000BASE-T

No.	Troubleshooting Steps	Problem	Action
1	According to the failure statistical information displayed by the <code>show interfaces</code> command, check to see if the statistical information below is counted for the port. If counted, see "Problem" and "Action" columns. <ul style="list-style-type: none"> • Link down 	Line quality is degraded.	Check to see if the cable type is correct. For the fiber optics type, see "Hardware Installation Guide."
			Check to see if MDI-X is selected for pin mapping in the case of the following: <ul style="list-style-type: none"> • The port setting is fixed. • The port setting is auto negotiations and auto MDIX function is disabled.
			Check the cable length. For the cable length, see "Hardware Installation Guide."
			Check to see if the cable is connected correctly.
			Replace with the connection interface supported by this system. For the connection interfaces supported by this system, see "Configuration Settings."
			Perform the line test on this system and confirm that there is no problem in the receiving function. See the execution results of the <code>no test interfaces (Ethernet)</code> command and follow the indicated actions. For the test type to be specified, see "6.1 Testing Line."
2	According to the receiving error statistical information displayed by the <code>show interfaces</code> command, check to see if the statistical information below is counted for the port. If counted, see "Problem" and "Action" columns. <ul style="list-style-type: none"> • CRC errors • Symbol errors 	Line quality is degraded.	Check to see if the cable type is correct. For the fiber optics type, see "Hardware Installation Guide."
			Check to see if MDI-X is selected for pin mapping in the case of the following: <ul style="list-style-type: none"> • The port setting is fixed. • The port setting is auto negotiations, and auto MDIX function is disabled.
			Check the cable length. For the cable length, see "Hardware Installation Guide."
			Check to see if the cable is connected correctly.
			Replace with the connection interface supported by this system. For the connection interfaces supported by this system, see "Configuration Settings."
			Perform the line test on this system and confirm that there is no problem in the receiving function. See the execution results of the <code>no test interfaces</code> command and follow the indicated actions. For the test type to be specified, see "6.1 Testing Line."
3	According to the failure statistical information displayed by the <code>show interfaces</code> command, check to see if the statistical information below is counted for the port. If counted, see "Problem" and "Action" columns. <ul style="list-style-type: none"> • MDI cross over changed 	Pin mapping of the cable is not correct.	Correct the pin mapping. For pin mapping, see the manual "Configuration Settings."
4	Check the line type/line speed for the port according to the "Port detail" information generated by the <code>show interfaces</code> command. If the line type/line speed is not correct, see the "Problem" and "Action" columns.	An incompatible cable is used.	Check to see if the cable type is correct. For the fiber optics type, see "Hardware Installation Guide."
		The values set for configuration commands <code>speed</code> and <code>duplex</code> are incompatible with the target system.	Use the same values as the remote system in configuration commands <code>speed</code> and <code>duplex</code> .

3. Troubleshooting Functional Failures in Operation

No.	Troubleshooting Steps	Problem	Action
5	According to the failure statistical information displayed by the <code>show interfaces</code> command, check to see if the statistical information below is counted for the port. If counted, see "Problem" and "Action" columns. <ul style="list-style-type: none"> Long frames 	Packets with invalid frame length are received.	Follow the jumbo frame setting on the remote system.
6	Check to see if statistics in the following is not counted by the <code>show qos queueing</code> command. If it is counted, see "Problem" and "Action" columns. <ul style="list-style-type: none"> discard_pkt 	Packets are being discarded.	Review the system maintenance using discard control and shaper.

3.4.4 Actions against Troubles on 1000BASE-X

If a trouble occurs on 1000BASE-X, follow the procedure below to isolate the problem.

1. Checking log
For the log, see the manual "Message Log Reference."
2. Isolating the problem according to the failure analysis method
Isolate the problem according to the failure analysis method listed below.

Table 3-10: Failure Analysis Method for Troubles on 1000BASE-X

No.	Troubleshooting Steps	Problem	Action
1	According to the failure statistical information displayed by the <code>show interfaces</code> command, check to see if the statistical information below is counted for the port. If counted, see "Problem" and "Action" columns. <ul style="list-style-type: none"> Link down Signal detect errors 	Line quality on receiving side is degraded.	<p>Check the type of fiber optics. For the fiber optics type, see "Hardware Installation Guide."</p> <p>Check the attenuation value if an optical attenuator is used. For the optical level, see "Hardware Installation Guide."</p> <p>Check the cable length. For the cable length, see "Hardware Installation Guide."</p> <p>Check to see if the cable is connected correctly. Check to see if end surfaces of the cable are dirty. If they are dirty, remove the dirt.</p> <p>Check to see if the transceiver is connected correctly.</p> <p>Use the same values as the remote system in configuration commands <code>speed</code> and <code>duplex</code>.</p> <p>Follow the segment standard on the remote system.</p> <p>Check to see if the optical level is correct. For the optical level, see "Hardware Installation Guide."</p> <p>Perform the line test on this system and confirm that there is no problem in the receiving function. See the execution results of the <code>no test interfaces</code> command and follow the indicated actions. For the test type to be specified, see "6.1 Testing Line."</p>

No.	Troubleshooting Steps	Problem	Action
2	<p>According to the receiving error statistical information displayed by the <code>show interfaces</code> command, check to see if the statistical information below is counted for the port.</p> <p>If counted, see "Problem" and "Action" columns.</p> <ul style="list-style-type: none"> • CRC errors • Symbol errors 	Line quality on receiving side is degraded.	<p>Check the type of fiber optics. For the mode, see "Hardware Installation Guide."</p> <p>Check the attenuation value if an optical attenuator is used. For the optical level, see "Hardware Installation Guide."</p> <p>Check the cable length. For the cable length, see "Hardware Installation Guide."</p> <p>Check to see if the cable is connected correctly. Check to see if end surfaces of the cable are dirty. If they are dirty, remove the dirt.</p> <p>Check to see if the transceiver is connected correctly.</p> <p>Use the same values as the remote system in configuration commands <code>speed</code> and <code>duplex</code>.</p> <p>Follow the segment standard on the remote system.</p> <p>Check to see if the optical level is correct. For the optical level, see "Hardware Installation Guide."</p> <p>Perform the line test on this system and confirm that there is no problem in the receiving function. See the execution results of the <code>no test interfaces</code> command and follow the indicated actions. For the test type to be specified, see "6.1 Testing Line."</p>
3	<p>According to the failure statistical information displayed by the <code>show interfaces</code> command, check to see if the statistical information below is counted for the port.</p> <p>If counted, see "Problem" and "Action" columns. [IP8800/S3600] [IP8800/S2400]</p> <ul style="list-style-type: none"> • TX fault 	Transceiver is faulty.	Replace the transceiver.
4	Check to see if the combination of transceivers is valid when using the 1 core optical cable such as 1000BASE-BX.	Combination of transceivers is invalid.	For 1000BASE-BX, use U type and D type transceivers in pairs. Check to see if the transceiver type is correct.
5	<p>According to the failure statistical information displayed by the <code>show interfaces</code> command, check to see if the statistical information below is counted for the port.</p> <p>If counted, see "Problem" and "Action" columns.</p> <ul style="list-style-type: none"> • Long frames 	Packets with invalid frame length are received.	Follow the jumbo frame setting on the remote system.
6	<p>Check to see if statistics in the following is not counted by the <code>show qos queueing</code> command. If it is counted, see "Problem" and "Action" columns.</p> <ul style="list-style-type: none"> • <code>discard_pkt</code> 	Packets are being discarded.	Review the system maintenance using discard control and shaper.

3.4.5 Actions against Troubles on 10GBASE-R

If a trouble occurs on 10GBASE-R, follow the procedure below to isolate the problem.

1. Checking log

For the log, see the manual "Message Log Reference."

3. Troubleshooting Functional Failures in Operation

2. Isolating the problem according to the failure analysis method

Isolate the problem according to the failure analysis method listed below.

Table 3-11: Failure Analysis Method for Troubles on 10GBASE-R

No.	Troubleshooting Steps	Problem	Action
1	<p>According to the failure statistical information displayed by the <code>show interfaces</code> command, check to see if the statistical information below is counted for the port. If counted, see "Problem" and "Action" columns.</p> <ul style="list-style-type: none"> • Signal detect errors • LOS of sync [IP8800/S6700] [IP8800/S6600] [IP8800/S6300] • HI BER [IP8800/S6700] [IP8800/S6600] [IP8800/S6300] • LF [IP8800/S6700] [IP8800/S6600] [IP8800/S6300] 	Line quality on receiving side is degraded.	Check the type of fiber optics. For the fiber optics type, see "Hardware Installation Guide."
			Check the attenuation value if an optical attenuator is used. For the optical level, see "Hardware Installation Guide."
			Check the cable length. For the cable length, see "Hardware Installation Guide."
			Check to see if the cable is connected correctly. Check to see if end surfaces of the cable are dirty. If they are dirty, remove the dirt.
			Check to see if the transceiver is connected correctly.
			For the transceiver, follow the segment standard on the remote system.
			Check to see if the optical level is correct. For the optical level, see "Hardware Installation Guide."
2	<p>According to the receiving error statistical information displayed by the <code>show interfaces</code> command, check to see if the statistical information below is counted for the port. If counted, see "Problem" and "Action" columns.</p> <ul style="list-style-type: none"> • CRC errors • Symbol errors 	Line quality on receiving side is degraded.	Check the type of fiber optics. For the fiber optics type, see "Hardware Installation Guide."
			Check the attenuation value if an optical attenuator is used. For the optical level, see "Hardware Installation Guide."
			Check the cable length. For the cable length, see "Hardware Installation Guide."
			Check to see if the cable is connected correctly. Check to see if end surfaces of the cable are dirty. If they are dirty, remove the dirt.
			Check to see if the transceiver is connected correctly.
			For the transceiver, follow the segment standard on the remote system.
			Check to see if the optical level is correct. For the optical level, see "Hardware Installation Guide."
Perform the line test on this system and confirm that there is no problem in the receiving function. See the execution results of the <code>no test interfaces</code> command and follow the indicated actions. For the test type to be specified, see "6.1 Testing Line."			

No.	Troubleshooting Steps	Problem	Action
3	According to the failure statistical information displayed by the <code>show interfaces</code> command, check to see if the statistical information below is counted for the port. If counted, see "Problem" and "Action" columns. [IP8800/S6700] [IP8800/S6600] [IP8800/S6300] <ul style="list-style-type: none"> RF 	Line quality on sending side is degraded.	<p>Check the type of fiber optics. For the fiber optics type, see "Hardware Installation Guide."</p> <p>Check the attenuation value if an optical attenuator is used. For the optical level, see "Hardware Installation Guide."</p> <p>Check the cable length. For the cable length, see "Hardware Installation Guide."</p> <p>Check to see if the cable is connected correctly. Check to see if end surfaces of the cable are dirty. If they are dirty, remove the dirt.</p> <p>Check to see if the transceiver is connected correctly.</p> <p>For the transceiver, follow the segment standard on the remote system.</p> <p>Check to see if the optical level is correct. For the optical level, see "Hardware Installation Guide."</p> <p>Perform the line test on this system and confirm that there is no problem in the sending function. See the execution results of the <code>no test interfaces</code> command and follow the indicated actions. For the test type to be specified, see "6.1 Testing Line."</p>
4	According to the failure statistical information displayed by the <code>show interfaces</code> command, check to see if the statistical information below is counted for the port. If counted, see "Problem" and "Action" columns. <ul style="list-style-type: none"> Long frames 	Packets with invalid frame length are received.	Follow the jumbo frame setting on the remote system.
5	Check to see if statistics in the following is not counted by the <code>show qos queueing</code> command. If it is counted, see "Problem" and "Action" columns. <ul style="list-style-type: none"> <code>discard_pkt</code> 	Packets are being discarded.	Review the system maintenance using discard control and shaper.

3.4.6 Communication Failure on Using PoE

If electricity is not provided when PoE is in use, isolate the problem using the failure analysis methods listed in the following table.

Table 3-12: Communication Failure Analysis Methods When PoE Is in Use

No.	Troubleshooting Steps and Command	Action
1	Check to see PoEStatus display on the port by the <code>show power inline</code> command.	<ul style="list-style-type: none"> PoEStatus indicates off Electricity is not provided. Go to No.2. PoEStatus indicates denied A shortage of electricity to the whole equipment occurs. Go to No.3. PoEStatus indicates faulty Electricity is unable to be provided to the connected equipment. Go to No.4.
2	Check to see if the port is shutdown.	<ul style="list-style-type: none"> The port is shutdown Use the <code>no shutdown</code> command. The port is not shutdown Check to see if Power receiving equipment is connected properly.

3. Troubleshooting Functional Failures in Operation

No.	Troubleshooting Steps and Command	Action
3	Check to see Threshold(W) and Allocate(W) by the <code>show power inline</code> command.	Because a value in Allocate(W) is larger than one in Threshold(W), electricity is not able to be provided. First, check to see the amount of power supply provided to the whole system, the amount of electrical power allocation to the ports, and power consumption of the ports. And then configure these items to adjust allocations.
4	Check to see if a fault occurs by the <code>show logging</code> command.	Power receiving equipment or connection cable might be faulty. <ul style="list-style-type: none"> When "0/x Supplying power was stopped by the overload detection." is indicated. Because overload is detected, electricity is not able to be provided. Check to see the power receiving equipment or the connection cables. If it is not recovered, change the type and length of the cables by seeing "Hardware Installation Guide." If devices providing PoE are connected with each other, disable the PoE function of the port by the <code>power inline</code> command.

3.4.7 Communication Failure on Using Link Aggregation

If communication is disabled or if degenerated operation is performed when link aggregation is in use, isolate the problem using the failure analysis methods listed in the following table.

Table 3-13: Communication Failure Analysis Methods When Link Aggregation Is in Use

No.	Troubleshooting Steps and Command	Action
1	Check the setting of failed link aggregation using the <code>show channel-group</code> command with "detail" parameter specified.	Check to see if the link aggregation mode matches that of the remote system. If the mode is different from that of the remote system, change the mode so that it will match that of the remote system. If the link aggregation mode matches that of the remote system, check to see if the LACP starting methods for both ports are set to "passive." If they are set to "passive," change the setting on either one of the ports to "active."

No.	Troubleshooting Steps and Command	Action
2	Check the setting of failed port status using the <code>show channel-group</code> command with "detail" parameter specified.	<p>Check the status of each port. If all ports in a link aggregation group are Down, the link aggregation group is also Down.</p> <p>Take the action below for the Down port depending on the Reason displayed.</p> <ul style="list-style-type: none"> • CH Disabled The link aggregation group is Disabled and Down. • Port Down The link is down. See "3.4 Network Interface Communication Failure." • Port Speed Unmatch Due to mismatch of the line speed on other ports in the link aggregation group, a degeneration has occurred. To avoid degeneration, match the speed on all ports in the link aggregation group. • Duplex Half The mode is Half and the degenerated status has occurred. To avoid degeneration, set the Duplex mode to Full. • Port Selecting Because the port aggregation conditions are being checked, the degeneration has occurred. Wait until the check completes. If the degeneration is not recovered though you wait for a while, check to see the operation status and settings of the remote system. • Waiting Partner Synchronization The system has finished the port aggregation condition check and is waiting for the synchronization of the connected port, so the degeneration has occurred. If recovery does not occur after a while, check the remote system operation status and settings. • Partner System ID Unmatch Partner System ID received from the connected port does not match the Partner System ID of the group. As a result, the degeneration has occurred. To avoid degeneration, check the remote system operation and wiring. • LACPDU Expired Since the valid LACPDU time from the connected port has expired, the port has degenerated. Check the LACPDU statistics using the <code>show channel-group statistics</code> command with "lACP" parameter specified. Also, check the remote system operation status. • Partner Key Unmatch Since Key received from the connected port does not match Partner Key of the group, the degeneration has occurred. To avoid degeneration, check the remote system operation and wiring. • Partner Aggregation Individual Since link aggregation disabled is received from the connected port, the degeneration has occurred. To avoid degeneration, check the remote system operation and settings. • Partner Synchronization OUT_OF_SYNC Since synchronization disabled is received from the connected port, the degeneration has occurred. (This occurs if configuration is changed on this system or the line is blocked on the remote system.) • Port Moved The connected port was connected with another port. Check the wiring. • Operation of Detach Port Limit Since the detached port limiting function is activated, the link aggregation group is Down.

3.5 Layer 2 Network Communication Failure

3.5.1 Layer 2 Communication by VLAN Is Disabled

If layer 2 communication is disabled when using VLAN, isolate the problem using failure analysis method listed in the following table.

(1) Checking VLAN status

Execute the `show vlan` command or execute the `show vlan` command with "detail" parameter specified and check the VLAN status. Check items for each VLAN function are listed below.

(a) Check items common to all VLAN functions

- Confirm that the VLAN setting for the port is correct.
- Confirm that the port has been set up with the compatible mode. If the expected port does not belong to the default VLAN (VLAN ID 1), check the setting below.
 - Confirm that a port VLAN other than VLAN ID 1 is not assigned for the access VLAN or native VLAN.
 - Confirm that the default VLAN setting is assigned for "allowed vlan" in the trunk port.
 - Confirm that a mirror port is not assigned for.
- Confirm that VLANs with the function enabled (such as VLAN authentication [static] of IEEE802.1X function, Web authentication [fixed VLAN mode], and MAC authentication) and VLANs with the function disabled are not in the same trunk port.

(b) Check items for protocol VLAN

If protocol VLAN is in use, execute `show vlan` and confirm that the protocol is set correctly.

```
# show vlan
:
VLAN ID:100   Type:Protocol based   Status:Up
  Protocol VLAN Information Name:ipv4
    EtherType:0800,0806   LLC: Snap-EtherType:
  Learning:On   Uplink-VLAN:           Uplink-Block:   Tag-Translation:
:
```

(c) Check items for MAC VLAN

- When using the MAC VLAN, execute the `show vlan mac-vlan` command to confirm that the MAC address that is allowed the VLAN communication is set up correctly. The value in the parentheses indicates the function that registers a MAC address.

[Function]

- static: MAC address that is set with configuration.
- dot1x: MAC address that is set with IEEE802.1X.
- wa: MAC address that is set with Web authentication.
- vaa: MAC address that is set with authentication VLAN.

```
# show vlan mac-vlan
:
VLAN ID:100   MAC Counts:4
  0012.e200.0001 (static)           0012.e200.00:02 (static)
  0012.e200.0003 (static)           0012.e200.00:04 (dot1x)
```

- Execute the `show vlan mac-vlan` command to confirm that the same MAC address on the layer 2 authentication has not been set up for different VLAN configuration. A MAC address with * (asterisk) means

that the identical MAC address is set in the configuration and is disabled.

```
# show vlan mac-vlan
:
VLAN ID:500      MAC Counts:4
  0012.e200.aa01 (static)      0012.e200.aa02 (static)
  0012.e200.aa03 (static)      0012.e200.aa04 (dot1x)
VLAN ID:600      MAC Counts:1
  * 0012.e200.aa01 (dot1x)
```

(2) Checking port status

- Execute the `show vlan` command with "detail" parameter specified, and confirm that the port is Up. If the port is Down, see "[3.4 Network Interface Communication Failure](#)."
- Confirm that the port is in the Forwarding status. If the port is in the Blocking status, the reason is shown in parentheses. Check the operation status of the function causing the problem.

[Cause]

VLAN: VLAN is specified to suspended.
 CH: Forwarding is suspended by link aggregation.
 STP: Forwarding is suspended by spanning tree.
 GSRP: Forwarding is suspended by GSRP.
 dot1x: Forwarding is suspended by IEEE802.1X.
 CNF: Forwarding is suspended due to inability of configuration setting.
 AXRP: Forwarding is suspended by Ring Protocol.

```
# show vlan detail
:
VLAN ID:100      Type:Protocol based  Status:Up
:
  Port Information
    0/1           Up   Forwarding      Untagged
    0/2           Up   Forwarding      Tagged
```

(3) Checking MAC address table

(a) Checking MAC address learning status

- Execute the `show mac-address-table` command to retrieve the information of the failed destination MAC address.

```
# show mac-address-table
MAC address      VLAN   Type      Port-list
0012.e22c.650c   10     Dynamic  0/1
0012.e22c.650b   1     Dynamic  0/2
```

- Take the action below according to the Type displayed.

[When Type displayed is Dynamic]

MAC address learning information may not be updated. Execute the `clear mac-address-table` command to clear old information. The old information can be also cleared by sending frames from the destination system.

[When Type displayed is Static]

Check the forwarding destination port configured using configuration command `mac-address-table static`.

[When Type displayed is Snoop]

See "[3.5.4 Multicast Relay by IGMP snooping Is Disabled](#)" and "[3.5.5 Multicast Relay by MLD snooping Is Disabled](#)."

3. Troubleshooting Functional Failures in Operation

[When Type displayed is Dot1x]

See ["3.12.1 Communication Failure on Using IEEE 802.1X."](#)

[When Type displayed is Wa]

See ["3.12.2 Communication Failure on Using Web Authentication."](#)

[When Type displayed is Macauth]

See ["3.12.3 Communication Failure on Using MAC Authentication."](#)

- Flooding is executed if the MAC address is not displayed.
 - IP8800/S6700, IP8800/S6600, and IP8800/S6300:
If the communication still has been blocked despite no display appears, check to see if learning is suspended by MAC address learning limitation. In addition, check to see if the threshold in the Storm Control function is not too low.
 - IP8800/S3600 and IP8800/S2400:
If the communication still has been blocked despite no display appears, check to see if the Suppress Port-to-Port Forwarding has been enabled. In addition, check to see if the threshold in the Storm Control function is not too low.

(b) Checking MAC address learning limitation **[IP8800/S6700] [IP8800/S6600] [IP8800/S6300]**

Execute the `show mac-address-table` command with "learning-counter" parameter specified to check the information of MAC address learning limitation for the port and the VLAN to be checked.

```
>show mac-address-table learning-counter port 1/1-6
Date 2005/09/21 20:00:57 UTC
Port counts:6
Port      Count  Maximum Threshold  Status
1/1       3      -                -
1/2      1000    1000             800  Learning
1/3       0      -                -
1/4       50     60              40   Stop learning <---1
1/5       45     60              40   Learning
1/6       0      60              40   Learning
>show mac-address-table learning-counter vlan
Date 2005/09/21 20:00:57 UTC
VLAN counts:4
ID        Count  Maximum Threshold  Status
1         3      -                -
100      1000    1000             800  Stop learning <---1
200       0      -                -    No learning <---2
4095     90     100              100  Learning
```

1. MAC address learning is suspended according to the MAC address learning limitation value. Frames from the unlearned source address are discarded without learning the MAC address. However, flooding is executed for frames of VLAN for which MAC address learning is suppressed.
2. Suppression of MAC address learning is set. Flooding is executed for received frames.

(4) Checking filtering/QoS

Certain packets may have been discarded by filtering, or packets may have been discarded through bandwidth monitoring, discarding control, or shaper of the QoS control. Check to see if the conditions of filtering and QoS control in the configuration have been set up correctly and if bandwidth monitoring, discarding control, or shaper has been set up appropriately for system operation. For the procedure, see ["3.23.1 Checking Filtering/QoS Setting Information."](#)

3.5.2 Failures on Using Spanning Tree

If the spanning tree function is in use and a layer 2 communication failure occurs or the spanning tree operation status does not comply with the network configuration, isolate the problem according to the analysis method listed below. For the multiple spanning trees, check for each CIST or MST instance. For example, read the CIST route bridge or the route

bridge for each MST instance for route bridge, when checking the route bridge.

Table 3-14: Spanning Tree Failure Analysis Method

No.	Troubleshooting Steps and Command	Action
1	Execute the <code>show spanning-tree</code> command for the failed spanning tree and check the protocol status of the spanning tree.	If shown as Enable, go to No. 2.
		When tree information is not displayed while Ring Protocol and PVST+ both are in use, go to No.7.
		If shown as Disable, the spanning tree is suspended. Check the configuration.
		Ring Protocol and multiple spanning tree both are used, go to No.8.
		Check to see if the number of PVST+s is within the conditions of accommodation.
2	Execute the <code>show spanning-tree</code> command for the failed spanning tree and check the bridge identifier of the route bridge for the spanning tree.	Go to No. 3 if the bridge identifier of the route bridge complies with the network configuration.
		Check the network configuration and configuration if the bridge identifier of the route bridge does not comply with the network configuration.
3	Execute the <code>show spanning-tree</code> command for the failed spanning tree and check the port status and the port role of the spanning tree.	Go to No. 4 if the spanning tree port status and port role comply with the network configuration.
		When the systems before Ver10.6 is used: If the port status of the port for which the loop guard function is defined is Blocking or Discarding, check to see if the port is a designated port. If the port is a designated port, delete the setting of the loop guard function.
		If the spanning tree port status and port role do not comply with the network configuration, check the neighboring system status and configuration.
4	Execute the <code>show spanning-tree statistics</code> command for the failed spanning tree and check BPDU sending and receiving on the failed port.	Check the BPDU sending/receiving counter. [Root port] Go to No. 5 if the BPDU receiving counter has been incremented. If not so, BPDU may have been discarded by filtering, or BPDU may have been discarded through bandwidth monitoring, discarding control, or shaper of the QoS control. See " 3.23.1 Checking Filtering/QoS Setting Information " to check for it. If no problem is found, check the neighboring system.
		[Designated port] Go to No. 5 if the BPDU sending counter has been incremented. Otherwise, see " 3.4 Network Interface Communication Failure. "
5	Execute the <code>show spanning-tree</code> command for the failed spanning tree with "detail" parameter specified, and check the received BPDU bridge identifier.	Confirm that the received BPDU route bridge identifier and sending bridge identifier comply with the network configuration. Otherwise, check the neighboring system status.
6	Check to see if the maximum number of failed spanning trees is within the accommodating conditions.	Set up the number within the range of the accommodating conditions. For the accommodating conditions, see "Configuration Settings."
7	Check to see if vlan-mapping is applied to the single VLAN that is to operate with PVST+.	If vlan-mapping of Ring Protocol is not applied to the target VLAN, configure it. In addition, if multiple VLANs are applied to the vlan-mapping, review the vlan-mapping and change it to a single VLAN.
8	Check to see if the vlan-mapping of VLANs to be operated with MST instances is the same as that of Ring Protocol.	If vlan-mapping of Ring Protocol is not applied to the target VLAN, adjust it to match the configuration of VLANs with multiple spanning tree enabled.

3.5.3 Failures on Using Ring Protocol

This subsection describes Autonomous Extensible Ring Protocol failure.

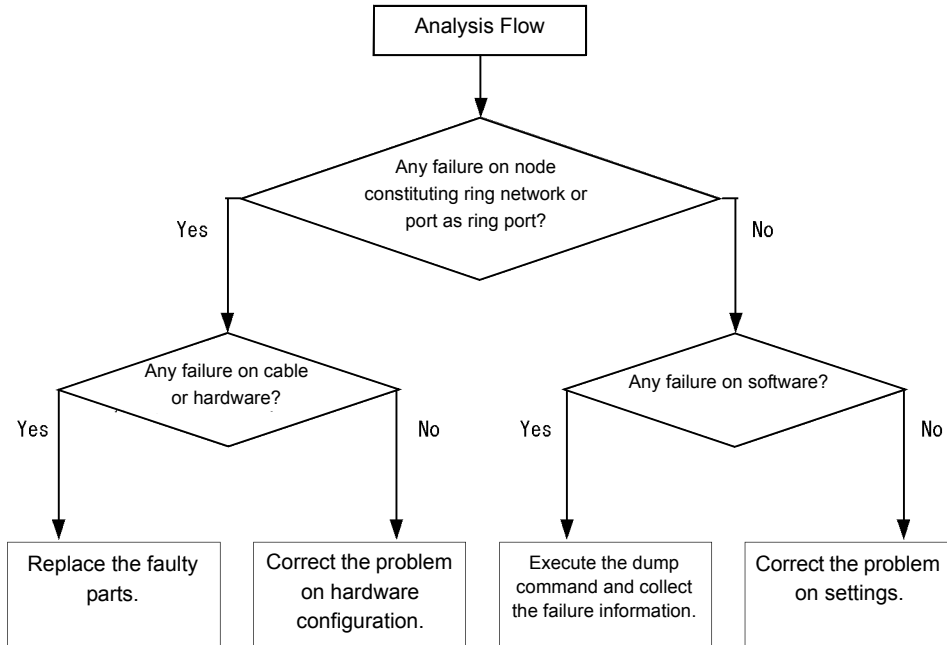
The Autonomous Extensible Ring Protocol is redundant protocol on the layer 2 network for ring topology, refer to it as "Ring Protocol" hereafter.

When the communication is disabled during Ring Protocol operation, follow the analysis flow to identify the symptom

3. Troubleshooting Functional Failures in Operation

and isolate the problem.

Figure 3-4: Analysis Flow



When the Ring Protocol is not running normally or the ring network failure is detected, isolate the problem by following the failure analysis methods shown in the table below for all the nodes configuring the ring network.

Table 3-15: Ring Protocol Failure Analysis Method

No.	Troubleshooting Steps and Command	Action
1	Execute the <code>show axrp</code> command to check the Ring Protocol operation state.	Go to No. 3 if "enable" is displayed on "Oper State." If "-" is displayed on "Oper State," the setting necessary for operating Ring Protocol is not set in the configuration. Check the configuration. If "disable" is displayed on "Oper State," Ring Protocol is disabled. Check the configuration. If "Not Operating" is displayed on "Oper State," Ring Protocol is inoperative. Check to see if any inconsistency (such as combination of operation mode, attribute and ring port of the system is invalid) exists in configuration. Go to No. 2 if configuration is valid. [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]
2	Execute the <code>show logging</code> command to check the normality of the entry registration to MAC address table as the default operation of Ring Protocol [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]	Go to No. 3 if the message "The MAC address entry can't be registered at hardware tables." is not output. If the message "The MAC address entry can't be registered at hardware tables." is output, the entry setting for MAC address table necessary for Ring Protocol operation is failed. See the corresponding part in the manual "Message Log Reference" and follow descriptions in [Action]. Also, see "4.1.2 Action to Be Taken When MAC Address Table Resource Shortage Occurs."
3	Execute the <code>show axrp</code> command to check the operation mode and attribute.	Go to No. 4 if "Mode" and "Attribute" correspond to the operation mode and attribute of network configuration. Otherwise, check the configuration.

No.	Troubleshooting Steps and Command	Action
4	Execute the <code>show axrp</code> command to check the ring port for each VLAN group and its operation state.	Go to No. 5 if "Ring Port" and "Role/State" correspond to the port state of network configuration. Otherwise, check the configuration.
5	Execute the <code>show axrp detail</code> command to check the control VLAN ID.	Go to No. 6 if "Control VLAN ID" corresponds to the VLAN ID of network configuration. Otherwise, check the configuration.
6	Execute the <code>show axrp detail</code> command to check the VLAN ID which belongs to the VLAN group.	Go to No. 7 if "VLAN ID" corresponds to the VLAN ID of network configuration. Otherwise, check the configuration.
7	Execute the <code>show axrp detail</code> command to check timer values for transmission interval and hold time of the health check frame.	Go to No. 8 if the timer value "Health Check Hold Time" of the health check frame hold time is larger than the timer value "Health Check Interval" of the health check frame transmission interval (i.e. transmission delay is considered). Check and review the configuration if the timer value of the health check frame hold time is equivalent or smaller than the that of health check frame transmission interval (i.e. transmission delay is not considered).
8	Execute the <code>show vlan detail</code> command to check the VLAN which is used in Ring Protocol and its port state.	Go to No. 9 and 10 if there is no failure on the VLAN and its port state. Check the configuration and restore the state if there is any failure.
9	Check settings of the filtering and QoS control.	Ring Protocol control frames may have been discarded by filtering or QoS control. See "3.23.1 Checking Filtering/QoS Setting Information" to check the setting. Also see the manual "Configuration Guide."
10	Check the settings of the virtual link if spanning tree or GSRP is used at the same time.	Check to see if virtual link has been correctly configured for the network configurations. <ul style="list-style-type: none"> • Check to see if the virtual link settings of devices that Ring Protocol and either one of spanning tree or GSRP are used together are correct. • As for equipment in the whole ring network, confirm the VLAN used as a virtual link belongs to the VLAN group of Ring Protocol.

3.5.4 Multicast Relay by IGMP snooping Is Disabled

If multicast relay is disabled when using IGMP snooping, follow the analysis flow to identify the symptom using steps shown in the table below and isolate the problem.

Figure 3-5: Analysis Flow

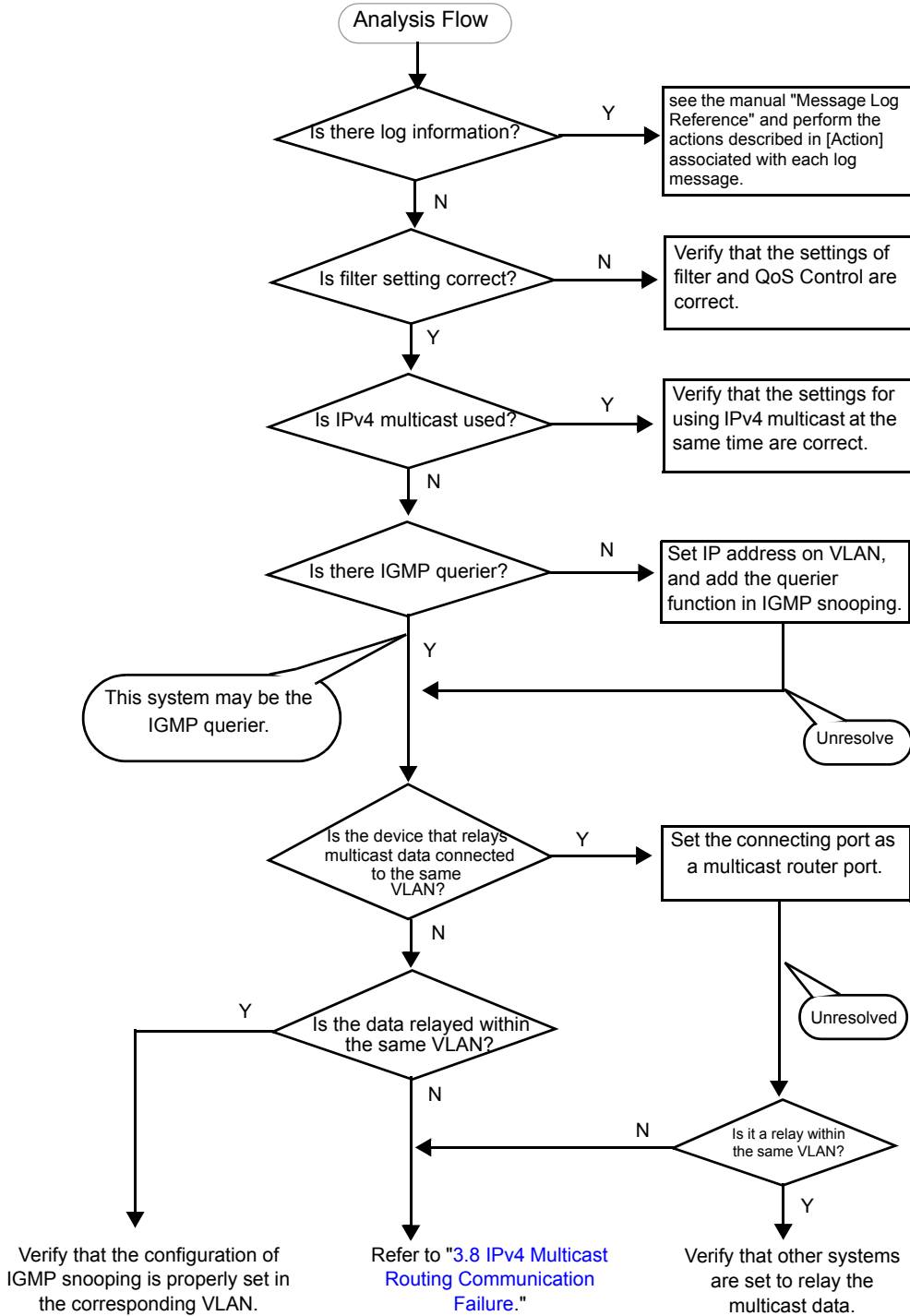


Table 3-16: Troubleshooting on Multicast Relay

No.	Troubleshooting Steps and Command	Action
1	Use the <code>show logging</code> command to check if any failure occurs.	Check the following: - Check the log information for physical failures.
2	Check if filtering and QoS are set correctly.	Certain packets may have been discarded by filtering, or packets may have been discarded through bandwidth monitoring, discarding control, or shaper of the QoS control. Check to see if the conditions of filtering and QoS control in the configuration have been set up correctly and if bandwidth monitoring, discarding control, or shaper has been set up appropriately for system operation. For the procedure, see " 3.23.1 Checking Filtering/QoS Setting Information. "
3	Check the settings of IPv4 multicasts if you want to use IPv4 multicast at the same time. [IP8800/S3600] [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]	<p>Check the following:</p> <ul style="list-style-type: none"> Check to see that the settings by configuration command <code>swrt_multicast_table</code> are applied to the system. [IP8800/S3600] <p>When the settings by configuration command <code>swrt_multicast_table</code> are applied, "On" is indicated on "Current selected <code>swrt_multicast_table</code>:" by entering the <code>show system</code> command.</p> <pre>Current selected swrt_multicast_table: On</pre> <p>When "Off" is indicated after the configuration command <code>swrt_multicast_table</code> has been executed, restart the system.</p> <ul style="list-style-type: none"> When IPv4 multicast and IGMP snooping are used at the same time, configure IPv4 multicast in the VLAN. [IP8800/S3600] <p>When IPv4 multicast is used in the VLAN, "On" is indicated in "IPv4 Multicast routing:" by entering the <code>igmp-snooping</code> command.</p> <pre>IPv4 Multicast routing: On</pre> <ul style="list-style-type: none"> When static group entry function of IPv4 multicast is used in the VLAN, set multicast router port to the ports that are necessary for multicast communication. When the number of entries registered in IGMP snooping exceeds the accommodation conditions, the excess multicast relay entries of IPv4 multicast can communicate only between multicast router ports. Therefore, set up the network configuration so as not to exceed the registered entries of IGMP snooping. <p>When the registered entries of IGMP snooping exceeds the accommodation conditions, log information is displayed in the following:</p> <pre>IGMP snooping: The number of the IGMP snooping entry exceeded the capacity of this system.</pre>

3. Troubleshooting Functional Failures in Operation

No.	Troubleshooting Steps and Command	Action
4	Check the IGMP snooping configuration using the <code>show igmp-snooping</code> command.	<p>Check the following:</p> <ul style="list-style-type: none"> - Check that the message below is displayed to confirm the existence of the IGMP querier which monitors group members. [IP8800/S3600] (1) If the IGMP querier exists, the IGMP querier IP address is displayed. <ul style="list-style-type: none"> IGMP querying system: 192.168.11.20* (2) If the IGMP querier does not exist, nothing is displayed in "IGMP querying system". <ul style="list-style-type: none"> IGMP querying system: - If this system is the IGMP querier, confirm that an IP address is set for the VLAN. <ul style="list-style-type: none"> (1) If an IP address is set for the VLAN, a message is displayed. <ul style="list-style-type: none"> IP Address: 192.168.11.20* (2) If no IP address is set for the VLAN, nothing is displayed in "IP Address:". <ul style="list-style-type: none"> IP Address: - If a multicast router is connected, check mrouter-port. <pre> > show igmp-snooping 100 Date 2005/05/15 15:20:00 VLAN 100: IP Address:192.168.11.20 Querier : enable IGMP querying system : 192.168.11.20 Port (2): 0/1,0/3 Mrouter-port:0/1 Group Counts: 3 </pre>
5	Execute the <code>show igmp-snooping</code> command with "group" parameter specified, and check IPv4 multicast group address.	<p>Check the following:</p> <ul style="list-style-type: none"> - Confirm that the joined IPv4 multicast group address is displayed by the <code>show igmp-snooping group</code> command. <pre> > show igmp-snooping group 100 Date 2005/05/15 15:20:00 VLAN 100 Group counts:3 Group Address MAC Address 224.10.10.10 0100.5e0a.0a0a Port-list 0/1-3 225.10.10.10 0100.5e0a.0a0a Port-list 0/1-2 239.192.1.1 0100.5e40.1606 Port-list 0/1 </pre>

* If this system is the IGMP querier, the address displayed in "IGMP querying system" matches the address displayed in "IP Address"; however, if a different system is the IGMP querier, the address displayed in "IGMP querying system" does not match the address displayed in "IP Address."

3.5.5 Multicast Relay by MLD snooping Is Disabled

If multicast relay is disabled when using MLD snooping, follow the analysis flow to identify the symptom using steps shown in the table below and isolate the problem.

Figure 3-6: Analysis Flow

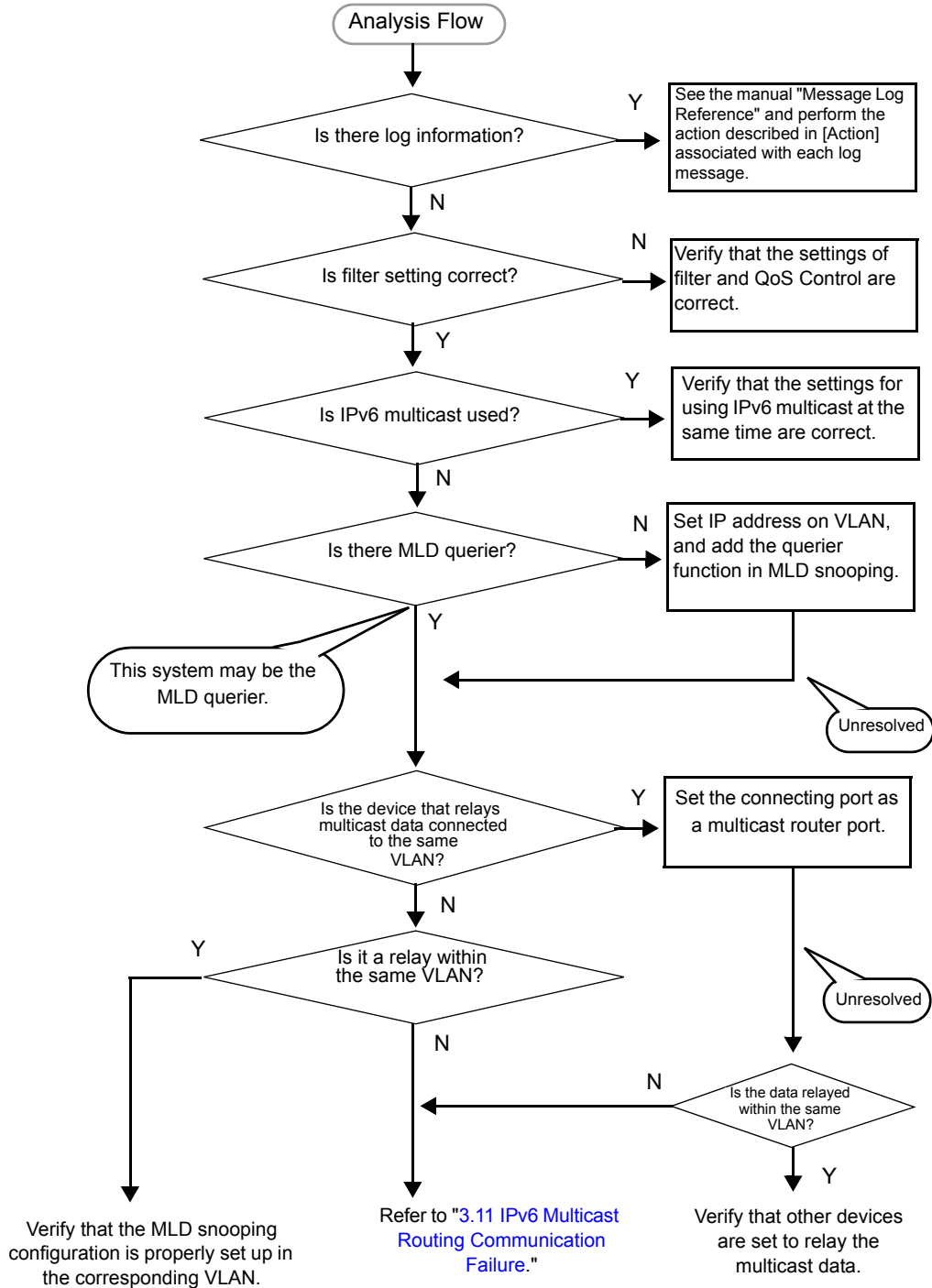


Table 3-17: Troubleshooting on Multicast Relay

No.	Troubleshooting Steps and Command	Action
1	Use the <code>show logging</code> command to check if any failure occurs.	Check the log information for physical failures.
2	Check if filtering and QoS are set correctly.	Certain packets may have been discarded by filtering, or packets may have been discarded through bandwidth monitoring, discarding control, or shaper of the QoS control. Check to see if the conditions of filtering and QoS control in the configuration have been set up correctly and if bandwidth monitoring, discarding control, or shaper has been set up appropriately for system operation. For the procedure, see "3.23.1 Checking Filtering/QoS Setting Information."
3	Check the settings of IPv6 multicasts if you want to use IPv6 multicast at the same time. [IP8800/S3600] [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]	<p>Check the following:</p> <ul style="list-style-type: none"> Check to see that the settings by configuration command are applied to the system [IP8800/S3600] <p>When the settings by configuration command <code>swrt_multicast_table</code> are applied, "On" is indicated on "Current selected swrt_multicast_table:" by entering the <code>show system</code> command.</p> <pre>Current selected swrt_multicast_table: On</pre> <p>When "Off" is indicated after the configuration command <code>swrt_multicast_table</code> has been executed, restart the system.</p> <ul style="list-style-type: none"> When IPv6 multicast and MLD snooping are used at the same time, configure IPv4 multicast in the VLAN. [IP8800/S3600] <p>When IPv6 multicast is used in the VLAN, "On" is displayed in "IPv4 Multicast routing:" by entering the <code>igmp-snooping</code> command.</p> <pre>IPv6 Multicast routing: On</pre> <ul style="list-style-type: none"> When static group entry function of IPv6 multicast is used in the VLAN, set multicast router port to the ports that are necessary for multicast communication. When the number of entries registered in MLD snooping exceeds the accommodation conditions, the excess multicast relay entries of IPv6 multicast can communicate only between multicast router ports. Therefore, set up network configuration so as not to exceed the registered entries of MLD snooping. <p>When the registered entries of MLD snooping exceeds the accommodation conditions, log information is displayed in the following:</p> <pre>MLD snooping: The number of the MLD snooping entry exceeded the capacity of this system.</pre>

No.	Troubleshooting Steps and Command	Action
4	Check the MLD snooping configuration using the <code>show mld-snooping</code> command.	<p>Check the following:</p> <ul style="list-style-type: none"> - Check that the message below is displayed to confirm the existence of the MLD querier which monitors group members. (1) If the MLD querier exists, the MLD querier IP address is displayed. <pre>MLD querying system: fe80::200:87ff:fe10:1959*</pre> (2) If the MLD querier does not exist, nothing is displayed in "MLD querying system". <pre>MLD querying system:</pre> - If this system is the MLD querier, confirm that an IP address is set for the VLAN. (1) If an IP address is set for the VLAN, the following message is displayed. <pre>IP Address: fe80::200:87ff:fe10:1959*</pre> (2) If no IP address is set for the VLAN, nothing is displayed in "IP Address:". <pre>IP Address:</pre> - If a multicast router is connected, check <code>mrouter-port</code>. <pre>>show mld-snooping 100 Date 2005/05/15 15:20:00 VLAN 100: IP Address:fe80::200:87ff:fe10:1959 Querier : enable MLD querying system: fe80::200:87ff:fe10:1959 Port(2): 0/1,0/3 Mrouter-port: 0/1 Group Count :3</pre>
5	Execute the <code>show mld-snooping</code> command with "group" parameter specified, and check IPv6 multicast group address.	<p>Check the following:</p> <ul style="list-style-type: none"> - Confirm that the joined IPv6 multicast group address is displayed by the <code>show mld-snooping group</code> command. <pre>> show mld-snooping group 100 Date 2005/05/15 15:20:00 VLAN 100 Group count:2 Group Address MAC Address ff0e::0e0a:0a01 3333.0e0a.0a01 Port-list 0/1-3 ff0e::0102:0c11 3333.0102.0c11 Port-list 0/1-2</pre>

* If this system is the MLD querier, the address displayed in "MLD querying system" matches the address displayed in "IP Address"; however, if a different system is the MLD querier, the address displayed in "MLD querying system" does not match the address displayed in "IP Address."

3.6 IPv4 Network Communication Failure

3.6.1 Communication Is Disabled or Is Disconnected

There are three possible causes that result in communication failure on the IPv4 network using this system.

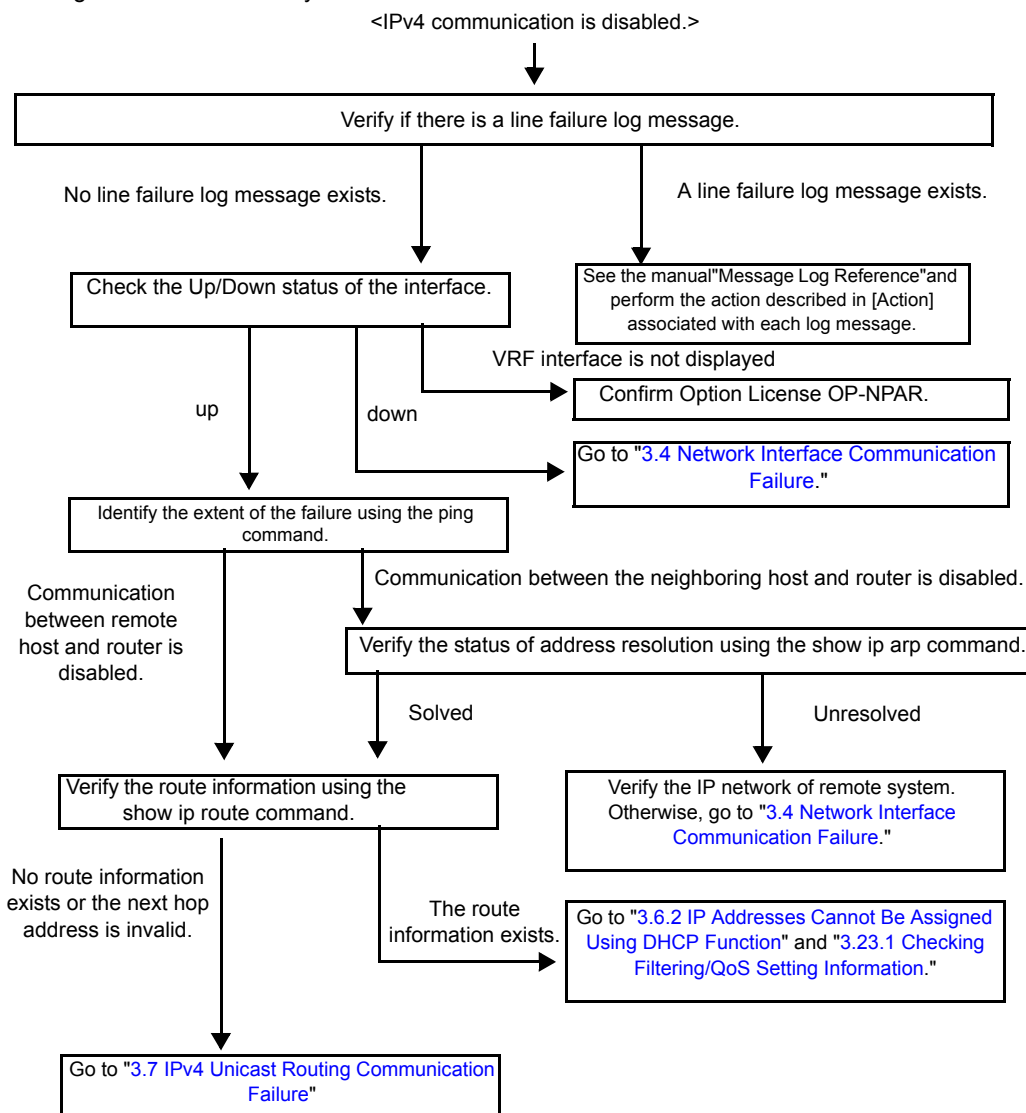
1. Configuration on IP communication has changed
2. Network configuration has changed
3. Network component failures

For 1 and 2 above, check for the differences in the configuration and network configuration provided before and after the change. Check for any difference disabling communication.

This section describes procedure to identify the failed part and to isolate the problem, mainly for the cases of "IP communication is disabled although the configuration and network configuration are correct." and "IP communication had been normally running but it is disabled now." as in above case 3.

To locate the faulty part and cause, follow the flow below.

Figure 3-7: Failure Analysis Procedure When IPv4 Communication Disabled



(1) Checking log

Communication may be interrupted by a line failure (or damage). The following procedure displays hardware error messages among this system's log messages.

For details about the log, see the manual "Message Log Reference."

1. Log in to the system.
2. Display the log using the `show logging` command.
3. The date and time when an error occurred are displayed in the log. Check to see if a log was displayed at the date/time when communication was disabled.
4. For detailed information about the failure in the log displayed at the time and date of the communication interruption and the actions for failures, see the manual "Message Log Reference." Follow the instruction.
5. If there is no log recorded at the time and date when communication was disabled, go to "(2)Checking interface status."

(2) Checking interface status

It is also possible that a failure has occurred on the hardware of the neighboring system connected to this system even if the hardware on this system is running properly.

The procedure for checking the status of interface between this system and the neighboring system is described below.

1. Log in to the system.
2. Check the Up/Down status of the interface between the systems using the `show ip interface` command.
3. When the interface is not displayed as VRF interface, see "[\(9\)Checking option license OP-NPAR \[OP-NPAR\].](#)" **[OP-NPAR]**
4. If the interface is in the "Down" status, see "[3.4 Network Interface Communication Failure.](#)"
5. If the interface is in the "Up" status, go to "[\(3\)Identifying the extent of the failure \(performed from this system\)](#)"

(3) Identifying the extent of the failure (performed from this system)

If no failure is found on this system, a failure may exist somewhere in the route between this system and the remote system. The procedure to locate the failure in the route to the remote system and identify the failure range is as follows:

1. Log in to the system.
2. Use the `ping` command to check communication between both parties. For an example of issuing `ping` and how to interpret the result, see the manual "Configuration Settings."
3. If communication to the other party cannot be verified with the `ping` command, use the `ping` command to check communication to remote systems starting from the system closest to this system.
4. If the result of the `ping` command shows that the neighboring system has failed, go to "[\(5\)Checking ARP resolution information with neighboring system.](#)" If the result shows that the remote system has failed, go to "[\(6\)Checking unicast routing information.](#)"

(4) Identifying the extent of failure (performed from the customer's terminal equipment)

If login to this system is not possible, follow the procedure below to identify the extent of failure to see the failure location in the route between the customer's terminal equipment and the other party.

1. Confirm that the customer's terminal equipment has the `ping` function.
2. Use the `ping` function to check communication between the customer's terminal equipment and the remote system.
3. If communication to the remote system cannot be verified with the `ping` command, use `ping` again to check communication to systems starting from the system closest to the customer's terminal equipment.
4. After the extent of failure has been identified using the `ping` command, log in to this system if it is considered to have failed and follow the failure analysis flow to check for the failure cause.

(5) Checking ARP resolution information with neighboring system

If communication to a neighboring system is not possible as a result of the `ping` command execution, address resolution by ARP may not have been achieved. The procedure for checking the status of address resolution between this system and the neighboring system is described below.

1. Log in to the system.
2. Use the `show ip arp` command to check the status of address resolution status with the neighboring system (presence/ absence of ARP entry information).
3. If the address resolution with the neighboring system is achieved (ARP entry information is provided), go to "[\(6\)Checking unicast routing information.](#)"
4. Confirm that the IP network setting on the neighboring system matches that of this system if the address resolution with the neighboring system is not achieved (ARP entry information is not provided).

(6) Checking unicast routing information

Check the route information acquired by this system if communication is not possible even when the address resolution with the neighboring system is achieved, or if communication is disabled in the midway to the other party during IPv4 unicast communication, or if the route to the other party is abnormal. Use the following procedure:

1. Log in to the system.
2. Execute the `show ip route` command to check the route information acquired by this system.
3. For IP8800/S6700, IP8800/S6600, and IP8800/S6300, check to see if packets are discarded because of the Null interface. If the route information sending interface resulting a communication failure is null0, packets are discarded because of the Null interface. Review the setting conditions for the static routing function in the configuration.
4. Go to "[3.7 IPv4 Unicast Routing Communication Failure](#)" if the route information on the failed interface is missing in the route information acquired by this system or if the next hop address is invalid.
5. If the route information acquired by this system contains the route information on the failed interface, the following functions set for the interface may have problem. Check these functions.
 - DHCP/BOOTP function
Go to "[\(7\)Checking DHCP/BOOTP setting information.](#)"
 - Filtering/QoS function
Go to "[\(8\)Checking filtering/QoS setting information.](#)"

(7) Checking DHCP/BOOTP setting information

When the relay function or the server function of DHCP/BOOTP on this system provides IP addresses to the neighboring system, there is possibility that IP addresses are not correctly assigned to the neighboring system.

Check to see the settings of the relay function or the server function. For the procedure, see "[3.23.1 Checking Filtering/QoS Setting Information.](#)"

(8) Checking filtering/QoS setting information

Certain packets may have been discarded by filtering, or packets may have been discarded through bandwidth monitoring, discarding control, or shaper of the QoS control. Review if the conditions of filtering and QoS control in the configuration have been set up correctly and if bandwidth monitoring, discarding control, or shaper has been set up appropriately for system operation. For the procedure, see "[3.23.1 Checking Filtering/QoS Setting Information.](#)"

(9) Checking option license OP-NPAR **[OP-NPAR]**

If no information is displayed by the `show ip interface` command though the interface is set to VRF interface and configured, there is possibility that option license OP-NPAR is unregistered or invalid. Check the status of option license on this system by using the `show license` command.

1. Log in to the system.
2. Check to see the license software and the enabled options by using the `show license` command.
3. If OP-NPAR does not appear in the license software, it indicates any license key for OP-NPAR has not been registered yet. Register the license key for OP-NPAR.
4. When OP-NAPR is displayed in license software but it is not displayed as an enabled option, the hardware configuration of this system might not support OP-NPAR. Review the hardware configuration. For more information about the hardware configuration, see the manual "Configuration Settings, Vol. 1."
5. When this system hardware configuration supports OP-NPAR but the OP-NPAR is not displayed as an enabled option, use the `reload` command to restart the system, which will enable the option license.
6. When OP-NPAR appears as an enabled option, see step 4 or later in "[\(2\)Checking interface status.](#)"

3.6.2 IP Addresses Cannot Be Assigned Using DHCP Function

(1) DHCP/BOOTP relay communication failure

There are three possible causes for DHCP/BOOTP relay communication failures:

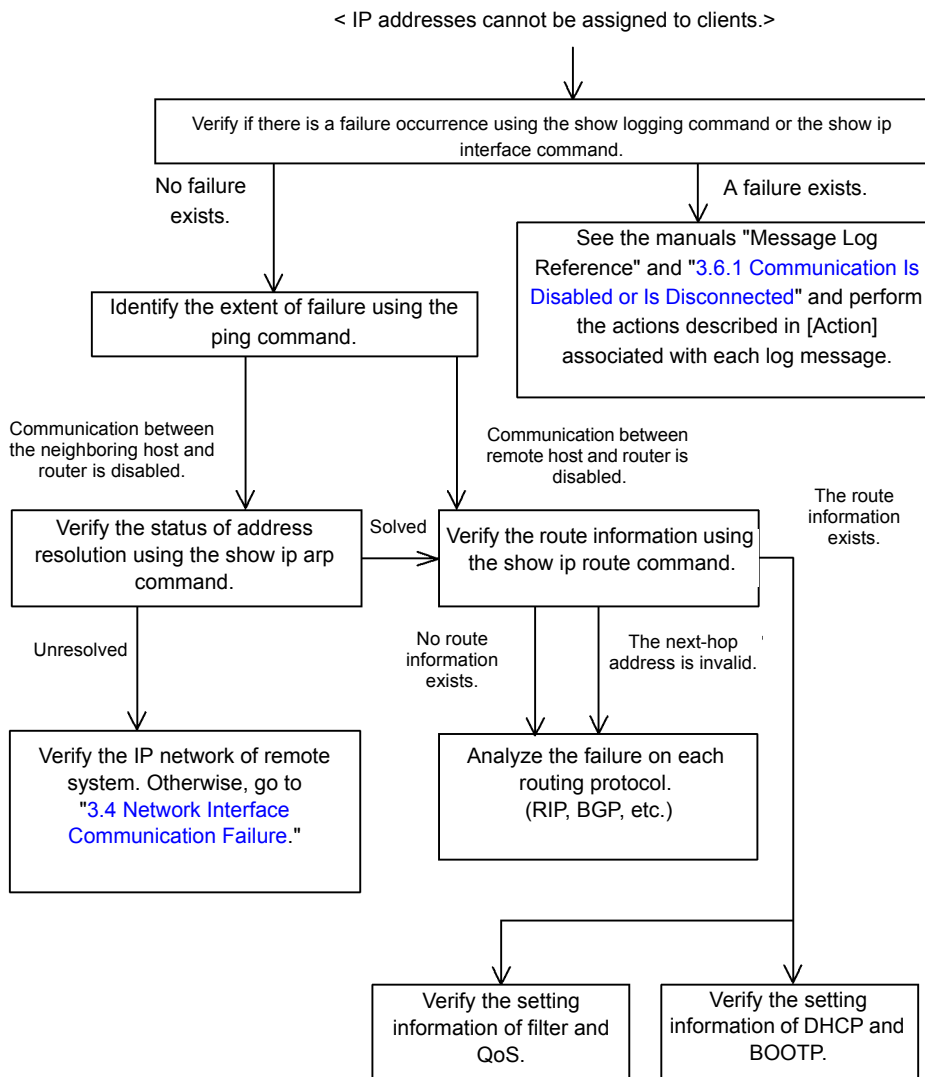
1. Configuration relating to DHCP/BOOTP relay has changed
2. Network configuration has changed
3. DHCP/BOOTP server failures

For 2 above, check for the differences in the network configuration provided before and after the change. Check for any difference disabling communication.

Assuming that client settings (network card setting, cable connection, etc.) have been verified, this section describes the procedure for locating the faulty part and cause in the cases described such as "IP addresses are not assigned from the DHCP/BOOTP server as a result of changing the configuration." and "Although the configuration and network configuration are correct, IP addresses are not assigned and IP communication is disabled" as in above No. 1 and 3.

To locate the faulty part and cause, follow the flow below.

Figure 3-8: Troubleshooting on DHCP/BOOTP Relay



(a) Checking the log and interface

On possible cause for the server not assigning IP addresses to clients, communication between client and server may have been disabled. Check the log displayed on this system or the interface up/down status using the `show ip interface` command. For the procedure, see "[3.6.1 Communication Is Disabled or Is Disconnected](#)."

(b) Identifying the extent of the failure (performed from this system)

If no failure is found on this system, a failure may exist somewhere in the route between this system and the remote system. The procedure to locate the failure in the route to the remote system and identify the failure range is as follows:

1. Log in to the system.
2. Use the `ping` command to check communication between both parties. For an example of issuing `ping` and how to interpret the result, see the manual "Configuration Settings."
3. If communication to the other party cannot be verified with the `ping` command, use the `ping` command to check communication to remote systems starting from the system closest to this system.
4. If the result of the `ping` command shows that the neighboring system has failed, go to "[\(d\)Checking ARP resolution information with neighboring system](#)." If the result shows that the remote system has failed, go to "[\(e\)Checking route information](#)."

(c) Identifying the extent of failure (performed from the customer's terminal equipment)

If login to this system is not possible, follow the procedure below to identify the extent of failure to see the failure location in the route between the customer's terminal equipment and the other party.

1. Confirm that the customer's terminal equipment has the `ping` function.
2. Use the `ping` function to check communication between the customer's terminal equipment and the remote system.
3. If communication to the remote system cannot be verified with the `ping` command, use `ping` again to check communication to systems starting from the system closest to the customer's terminal equipment.
4. After the extent of failure has been identified using the `ping` command, log in to this system if it is considered to have failed and follow the failure analysis flow to check for the failure cause.

(d) Checking ARP resolution information with neighboring system

If communication with a neighboring system is not possible as a result of `ping` execution, address resolution by ARP may not have been achieved. The procedure for checking the status of address resolution between this system and the neighboring system is described below.

1. Log in to the system.
2. Use the `show ip arp` command to check the status of address resolution status with the neighboring system (presence/ absence of ARP entry information).
3. If the address resolution with the neighboring system is achieved (ARP entry information is provided), go to "[\(e\)Checking route information](#)."
4. Confirm that the IP network setting can be exchanged between the neighboring system and this system if the address resolution with the neighboring system is not achieved (ARP entry information is not provided).

(e) Checking route information

Check the route information acquired by this system if the following happens: Communication is not possible even when the address resolution with the neighboring system is achieved, communication is disabled in the midway to the other party, or the route to the other party is abnormal.

Take the following procedure.

1. Log in to the system.

3. Troubleshooting Functional Failures in Operation

2. Execute the `show ip route` command to check the route information acquired by this system.
3. Go to "[3.7 IPv4 Unicast Routing Communication Failure](#)" if the route information on the failed interface is missing in the route information acquired by this system or if the next hop address is invalid.
4. If the route information acquired by this system contains the route information on the failed interface, the following functions set for the interface may have problem. Check these functions.
 - Filtering/QoS function
Go to "[\(f\)Checking filtering/QoS setting information.](#)"
 - DHCP/BOOTP function
Go to "[\(g\)Checking DHCP/BOOTP setting information.](#)"

(f) Checking filtering/QoS setting information

It may have been set to discard only certain packets by filtering, or packets may have been discarded through bandwidth monitoring, discarding control, or shaper of the QoS control.

Check to see if the conditions of filtering and QoS control in the configuration have been set up correctly and if bandwidth monitoring, discarding control, or shaper has been set up appropriately for system operation. For the procedure, see "[3.23.1 Checking Filtering/QoS Setting Information.](#)"

(g) Checking DHCP/BOOTP setting information

If there are sufficient lease IP addresses remaining in the DHCP/BOOTP server, IP addresses may not be assigned to clients due to configuration setting errors for the DHCP/BOOTP relay. The followings are the steps to check the configuration:

1. Confirm that the IP address of the DHCP/BOOTP server or that of a neighboring router with the DHCP/BOOTP relay agent function has been assigned for `ip helper-address`.
2. Confirm that `ip helper-address` has been assigned for the client interface.
3. Confirm that `ip bootp-hops` is set to a correct "bootp hops" value for the client.
4. For multi-homed configuration, confirm that the "ip relay-agent-address" value matches the IP address subnet distributed by the DHCP/BOOTP server.

(h) Checking when the DCCP relay and VRRP are operated on the same interface

If the DHCP/BOOTP relay and VRRP are operated on the same interface, the DHCP/BOOTP client gateway address (router option) must be set to the virtual router address specified in the VRRP configuration on the DHCP/BOOTP server. Otherwise, communication of the DHCP/BOOTP client may be disabled after master/standby router switching by VRRP. Follow the checking method for each DHCP/BOOTP server.

(2) DHCP server communication trouble

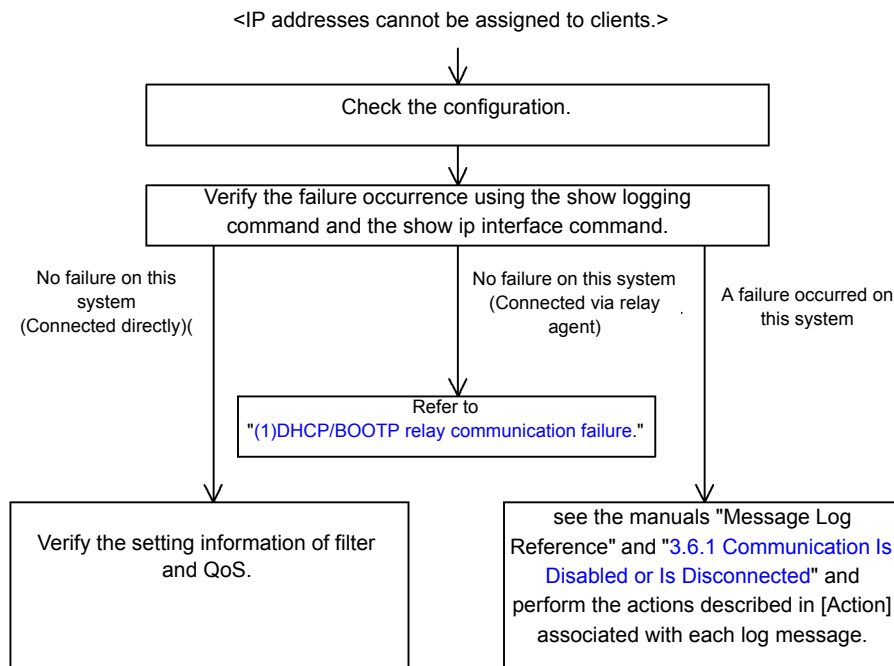
The following are three possible causes for DHCP server communication failures (address not distributed to clients).

1. Configuration error
2. Network configuration has changed
3. DHCP server failure

First, check 1 above. This section describes configurations that are easily misconfigured. For 2 above, check for the differences in the network configuration provided before and after the change. Check for any difference disabling communication. If the configuration and network configuration are correct but IP communications are unavailable because IP addresses cannot be assigned to clients, described in 3 above, see "[\(b\)Checking the log message and interface](#)" through "[\(e\)Checking filtering/QoS setting information](#)" for details.

To locate the failed part and cause, follow the flow below.

Figure 3-9: DHCP Server Failure Analysis Procedure

**(a) Checking configuration**

IP addresses may not be assigned to clients due to configuration setting errors for resources on the DHCP server. The followings are the steps to check the configuration:

1. Confirm that the configuration has the "ip dhcp pool" setting including the network setup of the IP address to be assigned to DHCP clients.
2. Using configuration command `ip dhcp excluded-address`, confirm that the number of pooled IP addresses in the configuration to be assigned to the DHCP clients is not fewer than the number of clients to be used concurrently.
3. If communication between a client and another system is disabled after an address is assigned by this system to the client, the default router may not have been set. Execute configuration command `default-router` to confirm that the router address (default router) of the network to which the client is connected has been set up (see the manual "Configuration Commands").
4. Check the setting of the system as the DHCP relay agent. If this system is also used as the relay agent, see "(1)DHCP/BOOTP relay communication failure."

(b) Checking the log message and interface

On possible cause for the server not assigning IP addresses to clients, the communication client between client and server may have been disabled. Check the log message displayed on this system or the interface up/down status using the `show ip interface` command. For the procedure, see "3.6.1 Communication Is Disabled or Is Disconnected."

(c) Identifying the extent of the failure (performed from this system)

If no failure is found on this system, a failure may exist somewhere in the route between this system and the remote system. The procedure to locate the failure in the route to the remote system and identify the failure range is as follows:

1. Log in to the system.
2. If a router is provided between the server and the client, use the `ping` command to verify communication of the system (router) between the server and the other system (DHCP client) to which communication is disabled. If

3. Troubleshooting Functional Failures in Operation

communication to the other party cannot be verified with the `ping` command, use `ping` to check communication toward clients starting from the system closest to this system. For an example of issuing `ping` and how to interpret the result, see the manual "Configuration Settings."

3. If the server and the client are directly connected, check the HUB and cable connections.
4. Depending on the extent of failure detected by the `ping` command, that is the neighboring system or remote system, proceed to the next step in the failure analysis flow.

(d) Checking route information

Check the route information acquired by this system if communication is not possible even when the address resolution with the neighboring system is achieved, or if communication is disabled in the midway to the other party, or if the route to the other party is abnormal. Use the following procedure:

1. Log in to the system.
2. Execute the `show ip route` command to check the route information acquired by this system.

(e) Checking filtering/QoS setting information

Only certain packets may have been discarded by filtering, or packets may have been discarded through bandwidth monitoring, discarding control, or shaper of the QoS control.

Check to see if the conditions of filtering and QoS control in the configuration have been set up correctly and if bandwidth monitoring, discarding control, or shaper has been set up appropriately for system operation in system configuration, on this system and on the relay equipment located between the client and server. For the procedure, see "[3.23.1 Checking Filtering/QoS Setting Information](#)."

(f) Checking layer 2 network

If no setting error or failure is found in steps (a) to (e), the layer 2 network may have problem. Check the layer 2 network, referring to "[3.5 Layer 2 Network Communication Failure](#)"

3.6.3 DynamicDNS Cooperation in DHCP Function Is Disabled

(1) DHCP server communication trouble

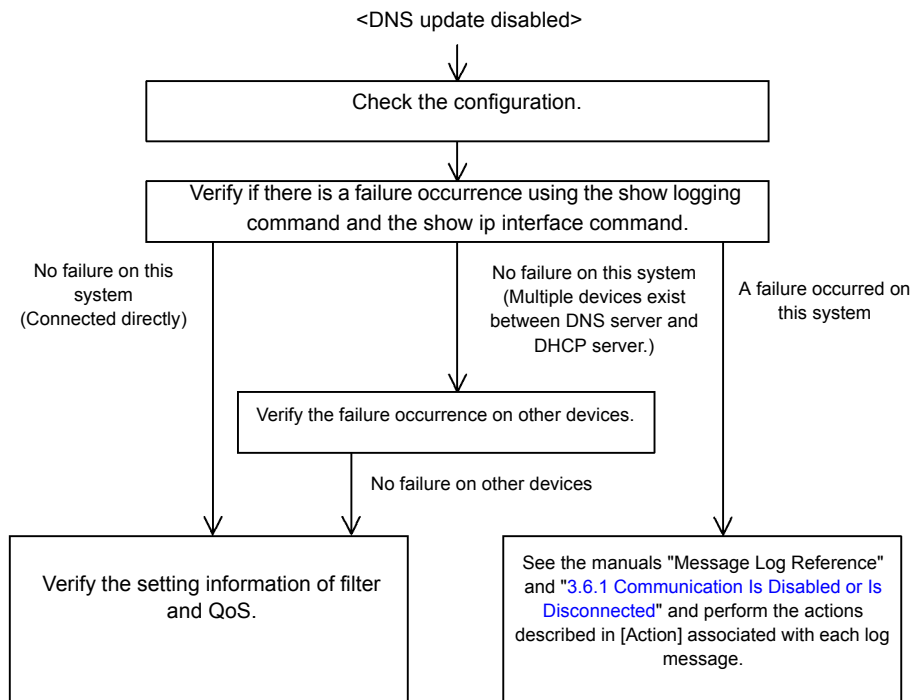
Following are three possible causes for DHCP server communication failures.

1. Configuration error
2. Network configuration has changed
3. DHCP server failure

First, check 1 above. This section describes configurations that are easily misconfigured. For 2 above, check for the differences in the network configuration provided before and after the change. Check for any difference disabling communication. If the DNS server/DHCP server settings (network card setting, cable connection, etc.) have been confirmed to be normal, and if the configuration and network configuration are correct but IP communications are unavailable because IP addresses cannot be assigned to clients, as described in 3 above, see "[\(b\)Checking time information](#)" through "[\(f\)Checking filtering/QoS setting information](#)" for details.

To locate the failed part and cause, follow the flow below.

Figure 3-10: Troubleshooting for DHCP Server Failure with DNS Cooperation

**(a) Checking configuration**

This failure may be caused by the incorrect DNS update on Dynamic DNS due to the DHCP server errors or the conflict with the settings on the DNS server. The followings are the steps to check the configuration:

1. First, check the method for permitting DNS update on the DNS server. For access permission with an IP address/network, see No. 3 and later. For permission with an authentication key, see No. 2 and later.
2. Confirm that the key information and authentication key specified on the DNS server are equivalent to the key information set in the DHCP server configuration (see the manual "Configuration Commands").
3. Confirm that the zone information specified on the DNS server is equivalent to the zone information in the DHCP server configuration (see the manual "Configuration Commands"). In this case, confirm that both forward lookup and reverse lookup are set.
4. Confirm that DNS update is defined (see the manual "Configuration Commands"). Since the DNS update is disabled by default, this setting is required to update DNS.
5. Confirm that the domain name used by the client matches the domain name registered on the DNS server. When distributing the domain name by DHCP, confirm that it is correctly set in the configuration (see "Configuration Commands" and "Operation Commands").

(b) Checking time information

When the authentication key is being used for DNS update, the difference in time between this system and the DNS server should be within 5 minutes as the UTC time in most cases. Use the show clock command to check the time information on this system and synchronize the time information referring to "Configuration Commands" and "Operation Commands," as required.

(c) Checking the log message and interface

As one of the causes for disabled communication to the DNS server, communication between the DNS server and DHCP server has been disabled. Check the log message displayed on this system or the interface up/down status using the show ip interface command. For the procedure, see "3.6.1 Communication Is Disabled or Is Disconnected."

(d) Identifying the extent of the failure (performed from this system)

If no failure is found on this system, a failure may exist somewhere in the route between this system and the remote system. The procedure to locate the failure in the route to the remote system and identify the failure range is as follows:

1. Log in to the system.
2. If a router is provided between the DNS server and DHCP server, use the `ping` command to verify communication of the system (router) between the DHCP server and the other system (DNS server) to which communication is disabled. If communication to the other party cannot be verified with the `ping` command, use `ping` to check communication toward clients starting from the system closest to this system. For an example of issuing ping and how to interpret the result, see the manual "Configuration Settings."
3. If the DNS server and DHCP server are directly connected, check the HUB and cable connections.
4. Depending on the extent of failure detected by the `ping` command, that is the neighboring system or remote system, proceed to the next step in the failure analysis flow.

(e) Checking route information

Check the route information acquired by this system if communication is not possible even when the address resolution with the neighboring system is achieved, or if communication is disabled in the midway to the other party, or if the route to the other party is abnormal. Use the following procedure:

1. Log in to the system.
2. Execute the `show ip route` command to check the route information acquired by this system.

(f) Checking filtering/QoS setting information

Only certain packets may have been discarded by filtering, or packets may have been discarded through bandwidth monitoring, discarding control, or shaper of the QoS control.

Check to see if the conditions of filtering and QoS control in the configuration have been set up correctly and if bandwidth monitoring, discarding control, or shaper has been set up appropriately for system operation in system configuration, on this system and on the relay equipment located between the DNS server and DHCP server. For the procedure, see "[3.23.1 Checking Filtering/QoS Setting Information](#)."

(g) Checking layer 2 network

If no setting error or failure is found in steps (a) to (f), the layer 2 network may have problem. Check the layer 2 network, referring to "[3.5 Layer 2 Network Communication Failure](#)."

3.7 IPv4 Unicast Routing Communication Failure

3.7.1 No RIP Routing Information Exists

Isolate the problem according to the failure analysis method listed below if RIP route information does not exist in the displayed route information acquired by this system.

Besides, when the upper limit of routing is set by configuration command `maximum routes`, see "[3.7.4 No Routing Information Exist \[OP-NPAR\].](#)" **[OP-NPAR]**

Table 3-18: RIP Failure Analysis Method

No.	Troubleshooting Steps and Command	Action
1	RIP neighboring information is displayed. <code>show ip rip neighbor</code>	Go to No. 2 if the interface of a neighboring router is not displayed.
		Go to No. 3 if the interface of a neighboring router is displayed.
2	Check to see if the RIP setting is correct in the configuration.	Go to No. 3 if the configuration is correct.
		Correct the configuration if it is not correct.
3	Confirm that the routing are not filtered by referring to the configuration.	Check to see if the neighboring router advertises the RIP route.
		Correct the configuration if it is not correct.

3.7.2 No OSPF Routing Information Exists

Isolate the problem according to the failure analysis method listed below if OSPF route information does not exist in the displayed route information acquired by this system.

Besides, when the upper limit of routing is set by configuration command `maximum routes`, see "[3.7.4 No Routing Information Exist \[OP-NPAR\].](#)" **[OP-NPAR]**

Table 3-19: OSPF Failure Analysis Method

No.	Troubleshooting Steps and Command	Action
1	Check the interface status of OSPF. <code>show ip ospf interface <IP Address></code>	Go to No. 3 if the interface status is DR.
		Go to No. 2 if the interface status is BackupDR or DR Other.
		Execute the command again after a certain period if the interface status is "Waiting." Go to No. 1.
2	Check the status of a neighboring router of DR from Neighbor List.	Go to No. 4 if the status of the neighboring router of DR is other than Full.
		Go to No. 5 if the status of the neighboring router of DR is Full.
3	Check the status of all neighboring routers from Neighbor List.	Go to No. 4 if the status of some neighboring routers is other than Full.
		Go to No. 5 if the status of all neighboring routers is Full.
4	Check to see if the OSPF setting is correct in configuration.	Go to No. 5 if the configuration is correct.
		Correct the configuration if it is not correct.
5	Check the OSPF routes that have been learned. <code>show ip route all-routes</code>	Go to No. 6 if the route is set to "Inactive."
		If no route exists, check to see if the neighboring router advertises the OSPF route.
6	Confirm that the routing are not filtered by referring to the configuration.	Check to see if the neighboring router advertises the OSPF route.
		Correct the configuration if it is not correct.

3.7.3 No BGP4 Routing Information Exists

Isolate the problem according to the failure analysis method listed below if BGP4 route information does not exist in the displayed route information acquired by this system.

Besides, when the upper limit of routing is set by configuration command `mazimum routes`, see "[3.7.4 No Routing Information Exist \[OP-NPAR\]](#)." **[OP-NPAR]**

Table 3-20: BGP4 Failure Analysis Method

No.	Troubleshooting Steps and Command	Action
1	Check the BGP4 peer status. <code>show ip bgp neighbors</code>	Go to No. 2 if the peer status is other than Established.
		Go to No. 3 if the peer status is Established.
2	Check to see if the BGP4 setting is correct in configuration.	Go to No. 3 if the configuration is correct.
		Correct the configuration if it is not correct.
3	Check to see if the BGP4 route is learned. <code>show ip bgp received-routes</code>	Go to No. 4 if the route does not exist.
		If the route exists, execute the <code>show ip route</code> command to confirm the learned route is active.
4	Check to see if the routing information exists to solve the next hop address. <code>show ip route</code>	If routing information exists to solve the next hop address, go to No.5.
		If no routing information exist to solve the next hop address, perform protocol fault analysis to learn the routing information.
5	Confirm that the routing are not filtered by referring to the configuration.	Check to see if the neighboring router advertises the BGP4 route.
		Correct the configuration if it is not correct.

3.7.4 No Routing Information Exist **[OP-NPAR]**

If no routing information for each protocol exist in the information this system acquired, isolate the cause according to the failure analysis method below.

Table 3-21: VRF Failure Analysis Method

No.	Troubleshooting Steps and Command	Action
1	Check to see if the number of routes in VRF exceeds the upper limit configured. <code>show ip vrf</code>	If the number of routes exceeds the upper limit, go to No.2.
		The number of routes is less than upper limit, perform protocol failure analysis against protocols that no routing information exists. RIP: " 3.7.1 No RIP Routing Information Exists " OSPF: " 3.7.2 No OSPF Routing Information Exists " BGP4: " 3.7.3 No BGP4 Routing Information Exists "
2	Check to see the value set in the upper limit for the number of routes in VRF in the configuration.	Increase the upper limit or aggregate the routing in order to decrease the routing number.

3.8 IPv4 Multicast Routing Communication Failure

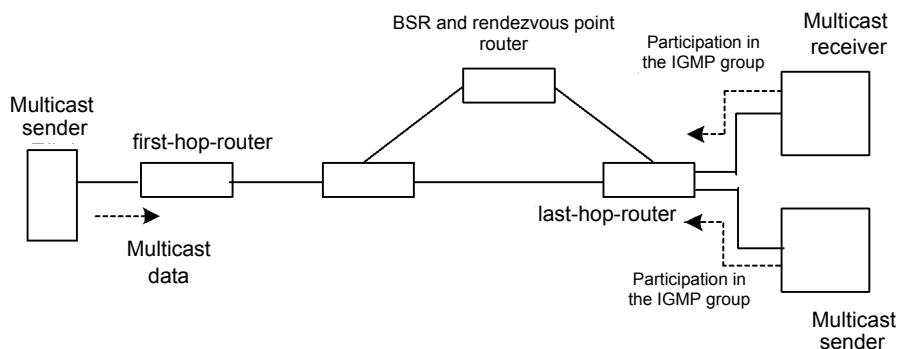
Actions to be taken if IPv4 multicast communication failures occur on this system are described below.

3.8.1 Communication on IPv4 PIM-SM Network Is Disabled

If multicast relay is disabled in the IPv4 PIM-SM network configuration, isolate the cause according to the failure analysis method below.

The figure below illustrates a network example of IPv4 PIM-SM.

Figure 3-11: Example of IPv4 PIM-SM Network



Note

- BSR: This router delivers rendezvous point information (for details, see the manual "Configuration Settings").
- Rendezvous point router: This router relays the packets, for which the relay destination is not determined, toward the multicast receiver (for details, see the manual "Configuration Settings").
- first-hop-router: This router is directly connected to the multicast sender.
- last-hop-router: This router is directly connected to the multicast receiver.

(1) Common check items

The table below shows the common check items for all system in the IPv4 PIM-SM network configuration.

Table 3-22: Common Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that the use of multicast function is designated (ip multicast routing) in the configuration. <code>show running-config</code>	If the use of multicast function is not designated, correct the configuration.
2	Confirm that PIM is running on one or more interfaces. <code>show ip pim interface</code>	If PIM is not running, check the configuration. Set PIM to run on one or more interfaces. If the interface set in the configuration to run PIM is not displayed by the <code>show ip pim interface</code> command, confirm that multi-homing is not set on the interface.
3	Check to see if IGMP snooping is applied to the interfaces with PIM enabled. <code>show igmp-snooping</code>	If IGMP snooping is applied, confirm the following: <ul style="list-style-type: none"> • Confirm the port to which the neighboring router connected is set as multicast router port of IGMP snooping. • See "3.5.4 Multicast Relay by IGMP snooping Is Disabled."

3. Troubleshooting Functional Failures in Operation

No.	Troubleshooting Steps and Command	Action
4	Confirm in the configuration that suppression of protocol packet and multicast packet relay through filtering, etc. is not provided on the interface that allows PIM and IGMP to run. <code>show running-config</code>	If suppression of protocol packet and multicast packet relay is provided, correct the configuration.
5	Check the PIM neighboring information. <code>show ip pim neighbor</code>	If the neighboring router is not displayed, check the following: <ul style="list-style-type: none"> • Confirm that PIM is running on the interface connected to the neighboring router using the <code>show ip pim interface</code> command. • Verify the settings of the neighboring router.
6	Check to see if the unicast route to the multicast data sender exists. <code>show ip route</code>	If the unicast route does not exist, see " 3.7 IPv4 Unicast Routing Communication Failure. "
7	Confirm that PIM is running on the interface to the next hop address for the multicast data sender. <code>show ip pim interface</code>	If PIM is not running, check the configuration. Set PIM to run on the interface connected to the next hop address for the multicast data sender.
8	Confirm that the PIM-SSM group addresses do not contain the relay target group address, referring to the configuration. <code>show running-config</code>	If the PIM-SSM group addresses contain the relay target group address, correct the configuration.
9	Confirm that BSR is determined. However, this confirmation is not required if the rendezvous point for the relay target group address is a static rendezvous point. <code>show ip pim bsr</code>	If BSR is not determined, check to see if the unicast route to BSR exists. If the unicast route does not exist, see " 3.7 IPv4 Unicast Routing Communication Failure. " If the unicast route exists, check the BSR setting. If the BSR is this system, see " (2)BSR check items. "
10	Confirm that the rendezvous point is determined. <code>show ip pim rp-mapping</code>	If the rendezvous point is not determined, check to see if the unicast route to the rendezvous point exists. If the unicast route does not exist, see " 3.7 IPv4 Unicast Routing Communication Failure. " If the unicast route exists, check the rendezvous point setting. If the rendezvous point is this system, see " (3)Rendezvous point router check items. "
11	Confirm that the rendezvous point group addresses contain the relay target group address. <code>show ip pim rp-mapping</code>	If the relay target group address is not contained, check the rendezvous point setting. If the rendezvous point is this system, see " (3)Rendezvous point router check items. "
12	Confirm that the multicast relay entry exists. <code>show ip mcache</code>	If the multicast relay entry does not exist, confirm that multicast data has arrived at the upstream port. If multicast data has not arrived, check the setting of the multicast sender or upstream router.
13	Confirm that the multicast relay routing information exists. <code>show ip mroute</code>	If the multicast routing information does not exist, check the setting of the downstream router.
14	Check to see if multicast routing information or multicast forwarding entry exceeds the upper limit. Multicast routing information: <code>show ip mroute</code> Multicast forwarding entry: <code>show ip mcache</code> <code>netstat multicast</code>	When warning is output, confirm that unexpected multicast routing information or unexpected multicast forwarding entry has not been created. If much of the negative cache exists in multicast forwarding entry, confirm that there is no terminal transmitting unnecessary packets.

(2) BSR check items

The table below shows the items to be checked when this system is BSR in the IPv4 PIM-SM network configuration.

Table 3-23: BSR Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that this system is a candidate for BSR. <code>show ip pim bsr</code>	If this system is not a candidate for BSR, check the configuration and set the configuration to run this system as a candidate for BSR. Since this system does not run as a candidate for BSR if no address is set for the loopback interface, confirm that an address is set for the loopback interface.
2	Confirm that this system is BSR. <code>show ip pim bsr</code>	If this system is not BSR, check the priority of other BSR candidates. The larger the value, the higher the priority. If the same priority is provided, the BSR candidate with the largest BSR address becomes BSR.

(3) Rendezvous point router check items

The table below shows the items to be checked when this system is the rendezvous point router in the IPv4 PIM-SM network configuration.

Table 3-24: Rendezvous Point Router Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that this system is a candidate of rendezvous point for the relay target group address. <code>show ip pim rp-mapping</code>	If this system is not a candidate of rendezvous point for the relay target group address, check the configuration and set the configuration to run this system as a candidate of rendezvous point for the relay target group address. Since this system does not run as a candidate of rendezvous point if no address is set for the loopback interface, confirm that an address is set for the loopback interface.
2	Confirm that this system is the rendezvous point for the relay target group address. <code>show ip pim rp-hash <Group Address></code>	If this system is not the rendezvous point, check the priority of other candidates of rendezvous point. The smaller the value, the higher the priority. If the priority of another candidate of rendezvous point is higher, this system does not run as the rendezvous point. If the same priority is provided, the rendezvous point is distributed for each group address according to the protocol specifications and this system may not run as the rendezvous point. To run this system preferentially as the rendezvous point, set the priority higher than those of other rendezvous point candidates.

(4) last-hop-router check items

The table below shows the items to be checked when this system is the last-hop-router in the IPv4 PIM-SM network configuration.

Table 3-25: last-hop-router Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that IGMP is running on the interface connected to the multicast receiver. <code>show ip igmp interface</code>	If IGMP is not running, check the configuration and set the configuration to run IGMP.
2	Confirm that the multicast receiver participates in the relay target group via IGMP. <code>show ip igmp group</code>	If the multicast receiver does not participate in the relay target group, check the setting of the multicast receiver.
3	If there is an interface in which the relay target group participates, confirm that this system is DR. <code>show ip pim interface</code>	If this system is not DR, check DR of the relay target interface.

3. Troubleshooting Functional Failures in Operation

No.	Troubleshooting Steps and Command	Action
4	Check to see if IGMP snooping is set to the port in which static group join function is working. <code>show igmp-snooping</code>	When IGMP snooping is set, confirm the following: <ul style="list-style-type: none"> • Confirm that relay port is set as multicast port for IGMP snooping • See "3.5.4 Multicast Relay by IGMP snooping Is Disabled."
5	Confirm that no interface in abnormal state is detected. <code>show ip igmp interface</code>	See notices and confirm that warning information is not output. When warning information is output, check the following: <ul style="list-style-type: none"> • L: The number of join request exceeded the maximum number expected. Check to see the number of connected users. • Q: The IGMP version of neighboring router is different. Adjust it to the same IGMP version. • R: A user who transmitted reports unreceivable at the present settings exists. Change the IGMP version of this system or confirm the settings of the participant. • S: Some of the participant information are being discarded because the number of source exceeded the upper limit defined to store source per message in IGMPv3. Check the settings of the participant.

(5) first-hop-router check items

The table below shows the items to be checked when this system is the first-hop-router in the IPv4 PIM-SM network configuration.

Table 3-26: first-hop-router Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that this system is directly connected to the multicast sender.	If not, check the network configuration.
2	Confirm that PIM or IGMP is running on the interface connected to the multicast sender. <code>show ip pim interface</code> <code>show ip igmp interface</code>	If PIM or IGMP is not running, check the configuration and set the configuration to run PIM or IGMP.
3	Confirm that the multicast relay routing information exists. <code>show ip mroute</code>	If the multicast routing information does not exist, confirm that multicast data source address is the network address of the interface directly connected to the multicast sender.

3.8.2 Multicast Data Is Double-relayed on IPv4 PIM-SM Network

If multicast data is double-relayed in the IPv4 PIM-SM network configuration, check the settings of each router and set the configuration to run PIM on the interface for a network having multiple routers.

If double-relay still continues, check the following:

Table 3-27: Check Items When Double-relay Continues

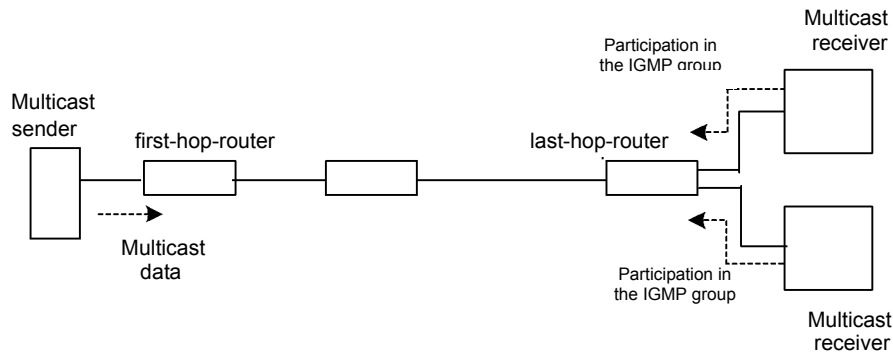
No.	Troubleshooting Steps and Command	Action
1	Check the PIM neighboring information on the interface of the network having multiple routers. <code>show ip pim neighbor</code>	If the neighboring router is not displayed, check the following: <ul style="list-style-type: none"> • Confirm that PIM is running on the interface connected to the neighboring router using the <code>show ip pim interface</code> command. • Confirm in the configuration that suppression of protocol packet relay by filtering, etc. is not provided. • Verify the settings of the neighboring router.

3.8.3 Communication on IPv4 PIM-SSM Network Is Disabled

If multicast relay on the IPv4 PIM-SSM network configuration is disabled, isolate the cause according to the failure analysis method below.

The figure below illustrates a network example of IPv4 PIM-SSM.

Figure 3-12: Example of IPv4 PIM-SSM Network



Note

- first-hop-router: This router is directly connected to the multicast sender.
- last-hop-router: This router is directly connected to the multicast receiver.

(1) Common check items

The table below shows the common check items for all system in the IPv4 PIM-SSM network configuration.

Table 3-28: Common Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that the use of multicast function is specified (ip multicast routing) in the configuration. <code>show running-config</code>	If the use of multicast function is not designated, correct the configuration.
2	Confirm that PIM is running on one or more interfaces. <code>show ip pim interface</code>	If PIM is not running, check the configuration. Set PIM to run on one or more interfaces. If the interface set in the configuration to run PIM is not displayed by the <code>show ip pim</code> command with "interface" parameter specified, confirm that multi-homing is not set on the interface.

3. Troubleshooting Functional Failures in Operation

No.	Troubleshooting Steps and Command	Action
3	Confirm that IGMP snooping is set to the interface with PIM enabled. <code>show igmp-snooping</code>	When the IGMP snooping is set, confirm the following: <ul style="list-style-type: none"> The port to which neighboring router connected is set as a multicast router port for IGMP snooping. See "3.5.4 Multicast Relay by IGMP snooping Is Disabled."
4	Confirm in the configuration that suppression of protocol packet and multicast packet relay through filtering, etc. is not provided on the interface that allows PIM and IGMP to run. <code>show running-config</code>	If suppression of protocol packet and multicast packet relay is provided, correct the configuration.
5	Check the PIM neighboring information. <code>show ip pim neighbor</code>	If the neighboring router is not displayed, check the following: <ul style="list-style-type: none"> Confirm that PIM is running on the interface connected to the neighboring router using the <code>show ip pim</code> command with "interface" parameter specified. Verify the settings of the neighboring router.
6	Check to see if the unicast route to the multicast data sender exists. <code>show ip route</code>	If the unicast route does not exist, see "3.7 IPv4 Unicast Routing Communication Failure."
7	Confirm that PIM is running on the sending interface for the unicast route to the multicast data sender. <code>show ip pim interface</code>	If IGMP is not running, check the configuration and set the configuration to run PIM on the sending interface for the unicast route.
8	Confirm that the PIM-SSM group addresses contain the relay target group address, referring to the configuration. <code>show running-config</code>	If the PIM-SSM group addresses do not contain the relay target group address, correct the configuration.
9	Confirm that the multicast relay routing information exists. <code>show ip mroute</code>	If the multicast routing information does not exist, check the setting of the downstream router.
10	Confirm that multicast routing information or multicast forwarding entry does not exceed the upper limit. Multicast routing information: <code>show ip mroute</code> multicast forwarding entry: <code>show ip mcache</code> <code>netstat multicast</code>	When warning is output, confirm that unexpected multicast routing information or unexpected multicast forwarding entry has not been created. If much of the negative cache exists in multicast forwarding entry, confirm that there is no terminal transmitting unnecessary packets.

(2) last-hop-router check items

The table below shows the items to be checked when this system is the last-hop-router in the IPv4 PIM-SSM network configuration.

Table 3-29: last-hop-router Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that the use of PIM-SSM cooperation in IGMPv1/IGMPv2 is designated (<code>ip igmp ssm-map enable</code>) in the configuration. <code>show running-config</code>	If the use of PIM-SSM cooperation in IGMPv1/IGMPv2 is not designated, correct the configuration.
2	Confirm in the configuration that PIM-SSM cooperation in IGMPv1/IGMPv2 is set (<code>ip igmp ssm-map static</code>) for the group address and source address to be relayed by PIM-SSM. <code>show running-config</code>	If PIM-SSM cooperation in IGMPv1/IGMPv2 is not set, correct the configuration.
3	Confirm that IGMP is running on the interface connected to the multicast receiver. <code>show ip igmp interface</code>	If IGMP is not running, check the configuration and set the configuration to run IGMP.
4	Confirm that the multicast receiver participates in the relay target group via IGMP. <code>show ip igmp group</code>	If the group does not participate in the relay target group, check the setting of the multicast receiver.

No.	Troubleshooting Steps and Command	Action
5	If there is an interface in which the relay target group participates, confirm that this system is DR. <code>show ip pim interface</code>	If this system is not DR, check DR of the relay target interface.
6	Confirm that IGMP snooping is set to the interface with static group join function enabled. <code>show igmp-snooping</code>	When the IGMP snooping is set, confirm the following: <ul style="list-style-type: none"> • Confirm that the relay port is set as a multicast router port for IGMP snooping. • See "3.5.4 Multicast Relay by IGMP snooping Is Disabled."
7	Confirm that no interface in abnormal state is detected. <code>show ip igmp interface</code>	See notices and confirm that warning information is not output. When warning information is output, check the following: <ul style="list-style-type: none"> • L: The number of join request exceeded expected maximum number. Check to see the number of connected users. • Q: The IGMP version of neighboring router is different. Adjust it to the version of IGMP. • R: A user who transmitted reports unreceivable at the present settings exists. Change the IGMP version of this system or confirm the setting of the participant. • S: Some of the participant information are being discarded because the number of source exceeded the upper limit defined to store source per message in IGMPv3. Check the settings of the participant.

(3) first-hop-router check items

The table below shows the items to be checked when this system is the first-hop-router in the IPv4 PIM-SSM network configuration.

Table 3-30: first-hop-router Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that this system is directly connected to the multicast sender.	If not, check the network configuration.
2	Confirm that PIM or IGMP is running on the interface connected to the multicast sender. <code>show ip pim interface</code> <code>show ip igmp interface</code>	If PIM or IGMP is not running, check the configuration and set the configuration to run PIM or IGMP.
3	Check to see if multicast data arrives at this system.	If multicast data has not arrived, check the setting of the multicast sender.
4	Check to see if the group address and source address in multicast data match those in the multicast routing information. <code>show ip mroute</code> <code>show netstat multicast</code>	If the group address and source address do not match, check the settings of the multicast sender and last-hop-router.

3.8.4 Multicast Data Is Double-relayed on IPv4 PIM-SSM Network

If multicast data is double-relayed in the IPv4 PIM-SSM network configuration, check the settings of each router and set the configuration to run PIM on the interface for a network having multiple routers.

If double-relay still continues, check the following:

Table 3-31: Check Items When Double-relay Continues

No.	Troubleshooting Steps and Command	Action
1	<p>Check the PIM neighboring information on the interface of the network having multiple routers.</p> <pre>show ip pim neighbor</pre>	<p>If the neighboring router is not displayed, check the following:</p> <ul style="list-style-type: none"> • Confirm that PIM is running on the interface connected to the neighboring router using the <code>show ip pim</code> command with "interface" parameter specified. • Confirm in the configuration that suppression of protocol packet relay by filtering, etc. is not provided. • Verify the settings of the neighboring router.

3.8.5 IPv4 Multicast Communication Failure In VRF [OP-NPAR]

If IPv4 multicast communication failure still continues, check the following:

Table 3-32: Check Items for VRF

No.	Troubleshooting Steps and Command	Action
1	<p>Check to see the VRF interface, port number, VLAN ID.</p> <pre>show ip vrf show vlan show ip pim interface</pre>	<p>If the setting is not correct, modify the configuration or the connections.</p>
2	<p>When this system operates as rendezvous point or BSR, confirm that loopback interface is set to the VRF or the configuration.</p> <pre>show ip vrf show running-config</pre>	<p>Specify the same loopback interface number between rendezvous point/BSR and the VRF.</p> <p>Besides, If IPv4 address is not set to the loopback interface, assign IPv4 address.</p>
3	<p>When multiple VRFs are operating, confirm that global network or a specific VRF does not occupy more multicast forwarding entries than expected.</p> <pre>show ip mcache vrf all</pre>	<p>If you find a specific global network or VRF that occupied more multicast forwarding entries than expected, check to see if unexpected multicast relay entry has not been created.</p> <p>If much of the negative cache exist in multicast forwarding entry, check to see if no terminal transmitting unnecessary packets exist. In addition, keep a global network or a specific VRF from occupying the forwarding entry.</p> <p>Corresponding Configuration:</p> <pre>ip pim vrf <vrf id> mcache-limit <number></pre>
4	<p>For each VRF, check the items from "3.8.1 Communication on IPv4 PIM-SM Network Is Disabled" to "3.8.4 Multicast Data Is Double-relayed on IPv4 PIM-SSM Network."</p>	<p>To confirm technical information by using commands, you need to specify VRF. For more information on how to specify VRF, see the manual "Operation Commands."</p>

3.9 IPv6 Network Communication Failure

3.9.1 Communication Is Disabled or Is Disconnected

There are three possible causes that result in communication failure on the IPv6 network using this system.

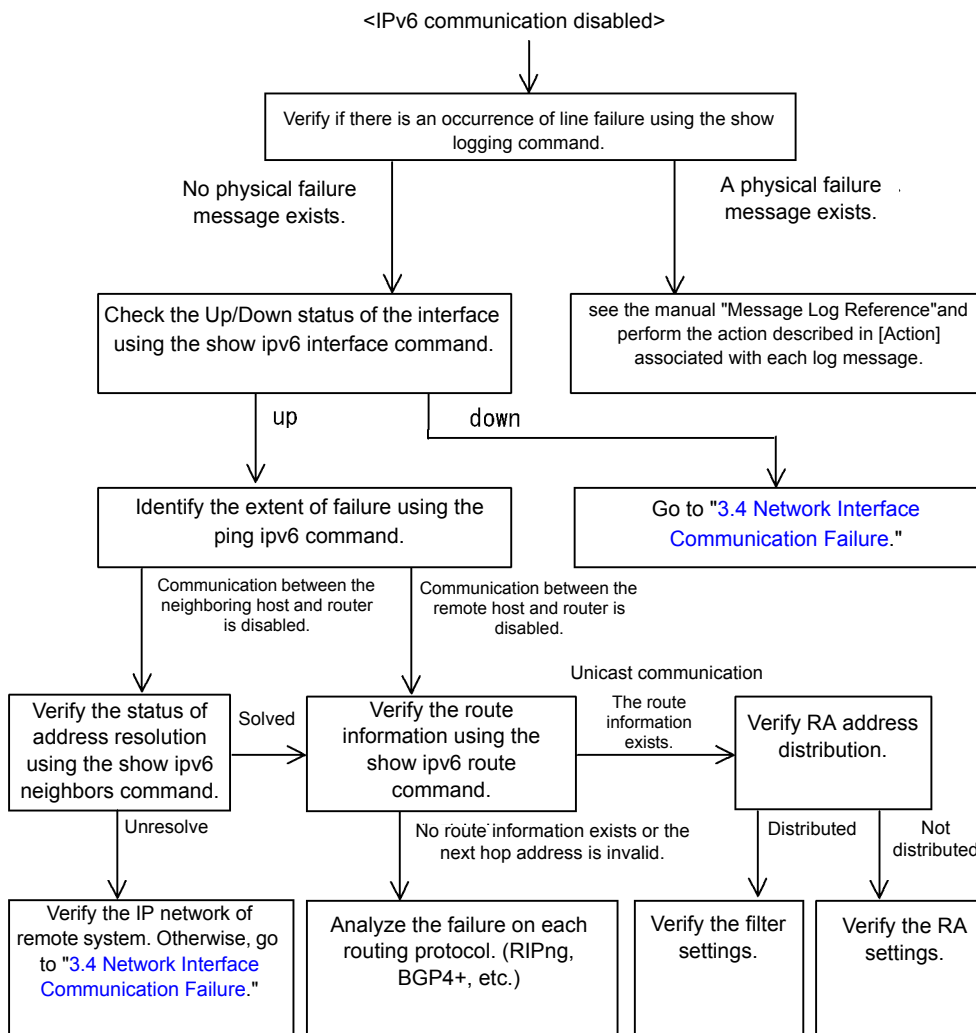
1. Configuration on IPv6 communication has changed
2. Network configuration has changed
3. Network component failures

For 1 and 2 above, check for the differences in the configuration and network configuration provided before and after the change. Check for any difference disabling communication.

This section describes procedure to identify the failed part and to isolate the problem, mainly for the cases of "IPv6 communication is disabled although the configuration and network configuration are correct." and "IPv6 communication had been normally running but it is disabled now." as described in 3 above.

To locate the faulty part and cause, follow the flow below.

Figure 3-13: Failure Analysis Procedure When IPv6 Communication Disabled



(1) Checking the log and interface

Communication may be interrupted by a line failure (or damage) or a neighboring system failure. Check the log displayed on this system or the interface up/down status using the `show ipv6 interface` command. For the procedure, see "[3.6.1 Communication Is Disabled or Is Disconnected.](#)"

(2) Identifying the extent of the failure (performed from this system)

If no failure is found on this system, a failure may exist somewhere in the route between this system and the remote system. The procedure to locate the failure in the route to the remote system and identify the failure range is as follows:

1. Log in to the system.
2. Use the `ping ipv6` command to check communication between both parties. For an example of issuing `ping ipv6` and how to interpret the result, see the manual "Configuration Settings."
3. If communication to the other party cannot be verified with the `ping` command, use `ping` to check communication to remote systems starting from the system closest to this system.
4. If the result of the `ping ipv6` command shows that the neighboring system has failed, go to "[\(4\)Checking NDP resolution information with neighboring system.](#)" If the result shows that the remote system has failed, go to "[\(5\)Checking unicast interface information.](#)"

(3) Identifying the extent of failure (performed from the customer's terminal equipment)

If login to this system is not possible, follow the procedure below to identify the extent of failure to see the failure location in the route between the customer's terminal equipment and the other party.

1. Confirm that the customer's terminal equipment has the `ping ipv6` function.
2. Use the `ping ipv6` function to check communication between the customer's terminal equipment and the remote system.
3. If communication to the remote system cannot be verified with the `ping ipv6` command, use `ping ipv6` again to check communication to systems starting from the system closest to the customer's terminal equipment.
4. After the extent of failure has been identified using the `ping ipv6` command log in to this system if it is considered to have failed and follow the failure analysis flow to check for the failure cause.

(4) Checking NDP resolution information with neighboring system

If communication to a neighboring system is not possible as a result of `ping ipv6` execution, address resolution by NDP may not have been achieved. The procedure for checking the status of address resolution between this system and the neighboring system is described below.

1. Log in to the system.
2. Use `show ipv6 neighbors` command to check the status of address resolution with the neighboring system (presence/absence of NDP entry information).
3. If the address resolution with the neighboring system is achieved (NDP entry information is provided), go to "[\(5\)Checking unicast interface information.](#)"
4. Confirm that the IP network setting on the neighboring system matches that of this system if the address resolution with the neighboring system is not achieved (NDP entry information is not provided).

(5) Checking unicast interface information

Check the route information acquired by this system if communication is not possible even when the address resolution with the neighboring system is achieved, or if communication is disabled in the midway to the other party during IPv6 unicast communication, or if the route to the other party is abnormal. Use the following procedure:

1. Log in to the system.
2. Execute `show ipv6 route` command to check the route information acquired by this system.
3. For IP8800/S6700, IP8800/S6600, and IP8800/S6300, check to see if packets are discarded because of the Null interface. If the route information sending interface resulting a communication failure is null0, packets are discarded because of the Null interface. Review the setting conditions for the static routing function in the configuration.
4. Go to "[3.9 IPv6 Network Communication Failure](#)" if the route information on the failed interface is missing in the route information acquired by this system or if the next hop address is invalid.
5. If the route information acquired by this system contains the route information on the failed interface, the following functions set for the interface may have problem. Check these functions.
 - RA function
Go to "[\(7\)Checking RA setting information](#)."

(6) Checking filtering/QoS setting information

Certain packets may have been discarded by filtering, or packets may have been discarded through bandwidth monitoring, discarding control, or shaper of the QoS control.

Review if the conditions of filtering and QoS control in the configuration have been set up correctly and if bandwidth monitoring, discarding control, or shaper has been set up appropriately for system operation in system configuration. For the procedure, see "[3.23.1 Checking Filtering/QoS Setting Information](#)."

(7) Checking RA setting information

If communication is not possible between this system and the terminal directly connected to this system, address information is not properly distributed by RA. Confirm that the RA function is set correctly in the configuration. Use the following procedure:

1. Log in to the system.
2. Execute the command `show ipv6 route` and check the RA information of this system.
3. If IPv6 address information is distributed properly, following function that is configured on the failed interface may have problem. Check these functions.
 - Filtering/QoS function
See "[\(8\)Checking filtering/QoS setting information](#)."

3.9.2 IPv6 DHCP Troubleshooting

(1) Configuration is not distributed

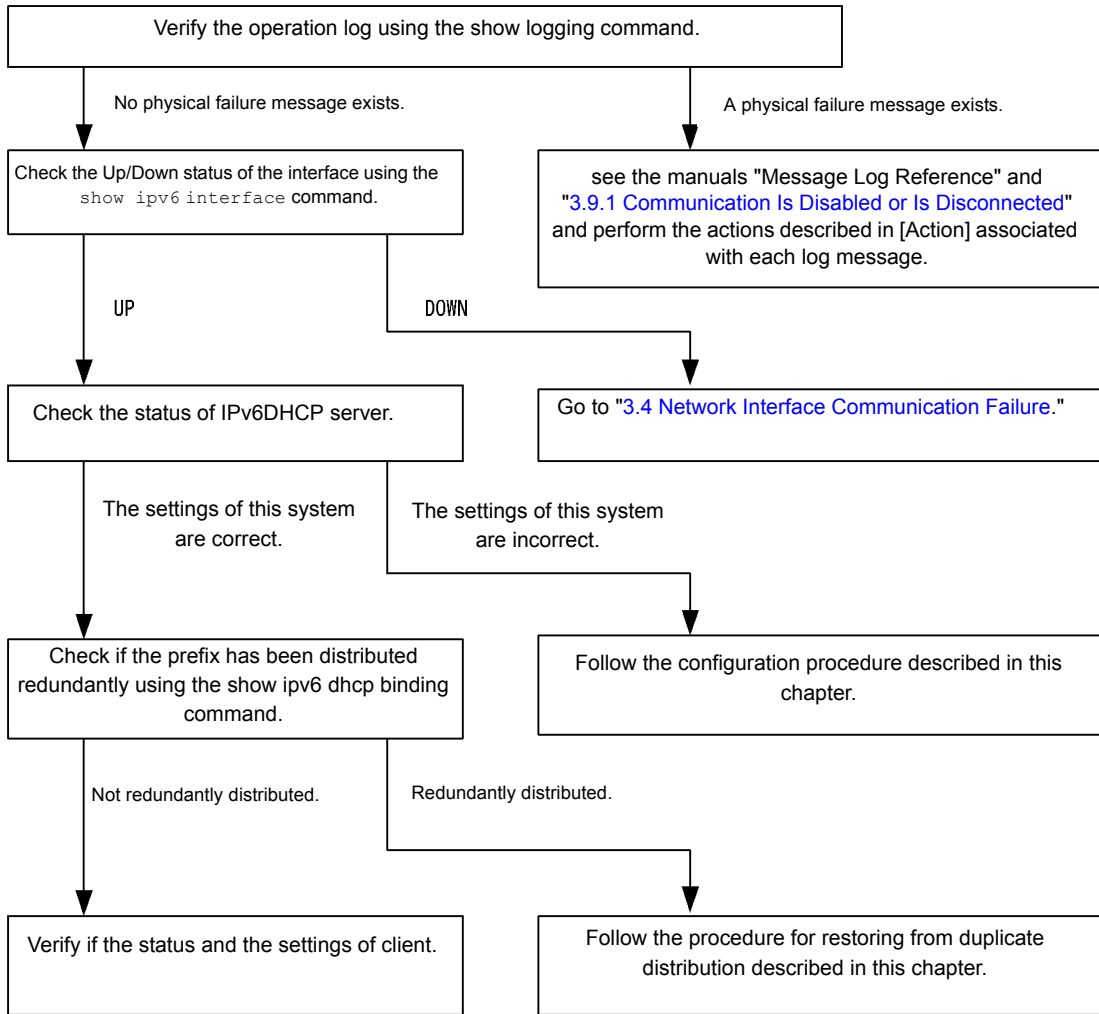
When using the prefix distribution feature of IPv6DHCP server in this system, the following five items are possible causes of service malfunction.

1. The client count is greater than the number of prefix that can be distributed.
2. The client DUID (DHCP Unique Identifier) is not correctly specified.
3. The "ipv6 dhcp server" setting is not correct.
4. Failure during IPv6DHCP operation
5. Other failures

The above problems can be isolated by determining the location of the failure using the following procedure.

Figure 3-14: IPv6DHCP Server Failure Analysis Procedure

<Unable to distribute the configuration.>



(a) Checking the log and interface

Communication may be interrupted by NIM or interface failure (or damage) or failure in the neighboring system. Check the log displayed by this system and the up/down status of interfaces using the `show inpv6 interface` command. For the procedure, see "3.9.1 Communication Is Disabled or Is Disconnected."

(b) Checking the status of the IPv6 DHCP server in this system

1. Checking if the IPv6DHCP server service is running

Confirm that information can be retrieved from the IPv6DHCP server daemon using the `show ipv6 dhcp server statistics` command. If the `show ipv6 dhcp server statistics` command produces the following output, reset IPv6DHCP server using configuration command `service ipv6 dhcp`.

[Execution results]

```
> show ipv6 dhcp server statistics
> < show statistics >: dhcp6_server doesn't seem to be running.
```

2. Checking the remaining distributable prefixes

Check the number of remaining prefixes that can be distributed from the IPv6DHCP server using the `show ipv6 dhcp server statistics` command. For the instructions, see "Configuration Settings." If the distributable number of prefixes is 0, increase the number of prefixes to be distributed. The prefixes can be distributed up to 1024.

(c) Procedure to check configuration

1. Confirm that IPv6DHCP server functions is enabled.

Execute configuration command `show service` to confirm that the "IPv6 DHCP" server is enabled. If the underlined part in the following results is not displayed, the "IPv6 DHCP" server is enabled.

```
[Execution results]
(config)# show service
no service ipv6 dhcp
!
(config)#
```

2. Checking "ipv6 dhcp server" setting.

Execute configuration command `show` to confirm that the "ipv6 dhcp server" setting presents. If not configured, add the configuration. If the setting presents, confirm that the specified interface supports the network on which clients are connected.

```
[Execution results]
(config)# show
interface vlan 10
  ipv6 address 3ffe:1:2:: linklocal
  ipv6 enable
  ipv6 dhcp server Tokyo preference 100
!
(config)#
```

3. Check the setting of ipv6 dhcp pool/ipv6 local pool/prefix-delegation/prefix-delegation pool.

Execute configuration command `show ipv6 dhcp` to confirm that the prefix distribution from the "IPv6DHCP" server is configured. If not configured, add the configuration. If this feature is configured, confirm that the value specified in "prefix-delegation/ipv6 local pool," which determine the prefix to be distributed, and presence/absence of "duid" configuration, which determine the target clients for the distribution, and the client DUID value defined in "duid" are correct.

```
[Execution results]
(config)# show ipv6 dhcp
ipv6 dhcp pool Tokyo
  prefix-delegation 3ffe:1:2::/48 00:03:00:01:11:22:33:44:55
!
(config)#
```

(d) Duplicate acquisition by the client

1. Checking binding information

Execute the `show ipv6 dhcp binding detail` command with "detail" parameter specified to confirm that only one prefix is distributed for each DUID. An example is as follows.

```
[Execution results]
> show ipv6 dhcp binding detail
Total: 2 prefixes
<Prefix>                <Lease expiration>  <Type>
<DUID>
3ffe:1234:5678::/48      05/04/01 11:29:00   Automatic
00:01:00:01:55:55:55:00:11:22:33:44:55
3ffe:aaaa:1234::/48     05/04/01 11:29:00   Automatic
00:01:00:01:55:55:55:00:11:22:33:44:55
>
```

As displayed in the underlined portion, if the same DUID appears two or more times, it may be a client that is improperly acquiring prefix information. Check each client and confirm the distributed prefixes value.

2. Matching distributed prefixes and clients

If no client is found that is acquiring duplicated prefixes as the results of the `show ipv6 dhcp binding`

3. Troubleshooting Functional Failures in Operation

detail command, it is necessary to match the displayed DUIDs and client systems. To do that, compare the value of distributed prefixes displayed in the binding information and the information of prefixes distributed to client system.

(e) Checking client setting

Check the client setting referring manuals provided with client.

(f) Procedure for restoring from duplicate distribution

If it is determined that duplicated prefixes were distributed to the same client by the IPv6DHCP server in this system, examine currently unused prefixes from the matching of displayed DUIDs and clients. Delete binding information for currently unused prefixes using the `clear ipv6 dhcp binding <unused prefixes>` command.

[Execution results]

```
> show ipv6 dhcp binding detail
Total: 2 prefixes
<Prefix>           <Lease expiration> <Type>
<DUID>
3ffe:1234:5678::/48 05/04/01 11:29:00 Automatic
00:01:00:01:55:55:55:55:00:11:22:33:44:55
3ffe:aaaa:1234::/48 05/04/01 11:29:00 Automatic
00:01:00:01:55:55:55:55:00:11:22:33:44:55
> clear ipv6 dhcp binding 3ffe:1234:5678::/48
> show ipv6 dhcp binding detail
<Prefix>           <Lease expiration> <Type>
<DUID>
3ffe:aaaa:1234::/48 05/04/01 11:29:00 Automatic
00:01:00:01:55:55:55:55:00:11:22:33:44:55
>
```

(2) Communication with the target of the prefix distribution is disabled

The following two possible causes of route information are not set when using the automatic route information setting feature for the route to prefix distribution target of the DHCP server in this system.

1. Information is configured but not distributed.
2. Operations or events have occurred that have an effect on functions relating to automatic route information setting.

It is possible to isolate the above reasons by comparing the results of the `show ipv6 route -s` command which checks route information and distributed prefix information displayed by the `show ipv6 dhcp server binding` command.

Table 3-33: Isolating Problems Relate Routing Information to Prefix Distribution Target

Condition		Cause
Binding Information	Route Information	
Yes	Route exists	Not applicable. active state.
Yes	No route	Cause 2
None	Route exists	Cause 2
None	No route	Causes 1, 2

There are limits to the retention of route information to prefix distribution target, as indicated in the table below.

Table 3-34: Retention of Route Information to Prefix Distribution Target

Retention Information Concerning Prefix	Event and Retention			
	Server Function Restart		Routing Manager Restart	This System Restart
	Command Execution	Server Failure		
Route information to client	Y	Y/N	Y	N

(Legend)

Y: Guaranteed

Y/N: Not guaranteed (each status information may be retained)

N: Not guaranteed (re-setting required because of initialization)

Note

Route management functions required when setting route information to prefix distribution target.

For other failures, see "3.9.1 Communication Is Disabled or Is Disconnected."

(a) Checking route information

When using the automatic route setting feature to the prefix distribution targets from the IPv6DHCP server, the route information after prefix distribution can be checked using the `show ipv6 route` command with "-s" parameter specified.

Figure 3-15: Check for Routing Information Using Operation Command

```
> show ipv6 route -s
Total: 10routes
Destination      Next Hop      Interface      Metric  Protocol  Age
3ffe:1234:5678::/48  ::1          tokyo          0/0     Static    45m
    <Active Gateway Dhcp>
3ffe:aaaa:1234::/48  ::1          osaka          0/0     Static    23m
    <Active Gateway Dhcp>
:
>
```

(b) Reconfiguring route information

When using automatic route information setting feature of the IPv6DHCP server of this system to prefix distribution target, if an event occurs that deletes route information due to a failure, etc., restoration requires the redistribution of prefixes. Execute operations for the re-acquisition of prefix information by the client system.

(3) If DUID of this system conflicts with other system

If DUID conflicts in the configurations with 2 or more IPv6DHCP servers including this system in the same network, reconfigure the DUID in this system according to the following procedure.

(a) Deleting the file containing DUID information

The DUID of this system is stored in `/usr/var/dhcp6/dhcp6s_duid`. Explicitly delete the file from the operation command line using `rm`.

(b) Reproducing the DUID

After deleting the DUID file, restart the server using the `restart ipv6 dhcp server` command or add an IPv6DHCP server setting to the configuration information. The IPv6DHCP server acquires the MAC address of the IPv6 interface used as IPv6DHCP server interface when restarted and generates new DUID based on that information and time information.

3. Troubleshooting Functional Failures in Operation

(c) Checking the DUID

You can check the DUID in the "< Server DUID >" section of the output of the `show ipv6 dhcp server statistics` command. For details, see "Configuration Settings."

3.10 IPv6 Unicast Routing Communication Failure

3.10.1 No RIPng Routing Information Exists

Isolate the problem according to the failure analysis method listed below if RIPng route information does not exist in the displayed route information acquired by this system.

Table 3-35: Failure Analysis of RIPng

No.	Troubleshooting Steps and Command	Action
1	RIPng neighboring information is displayed. <code>show ipv6 rip neighbor</code>	Go to No. 2 if the interface of a neighboring router is not displayed.
		Go to No. 3 if the interface of a neighboring router is displayed.
2	Check to see if the RIPng setting is correct in configuration.	Go to No. 3 if the configuration is correct.
		Correct the configuration if it is not correct.
3	Confirm that the routing are not filtered by referring to the configuration.	Check to see if the neighboring router advertises the RIPng route.
		Correct the configuration if it is not correct.

3.10.2 No OSPFv3 Routing Information Exists

Isolate the problem according to the failure analysis method listed below if OSPFv3 route information does not exist in the displayed route information acquired by this system.

Table 3-36: Failure Analysis of OSPFv3

No.	Troubleshooting Steps and Command	Action
1	Check the interface status of OSPFv3. <code>show ipv6 ospf interface <Interface Name></code>	Go to No. 3 if the interface status is DR.
		Go to No. 2 if the interface status is BackupDR or DR Other.
		Execute the command again after a certain period if the interface status is "Waiting." Go to No. 1.
2	Check the status of a neighboring router of DR from Neighbor List.	Go to No. 4 if the status of the neighboring router of DR is other than Full.
		Go to No. 5 if the status of the neighboring router of DR is Full.
3	Check the status of all neighboring routers from Neighbor List.	Go to No. 4 if the status of some neighboring routers is other than Full.
		Go to No. 5 if the status of all neighboring routers is Full.
4	Check to see if the OSPFv3 setting is correct in configuration.	Go to No. 5 if the configuration is correct.
		Correct the configuration if it is not correct.
5	Check the OSPFv3 routes that have been learned. <code>show ipv6 route all-routes</code>	Go to No. 6 if the route is set to "Inactive."
		If no route exists, check to see if the neighboring router advertises the OSPFv3 route.
6	Confirm that the routing are not filtered by referring to the configuration.	Check to see if the neighboring router advertises the OSPFv3 route.
		Correct the configuration if it is not correct.

3.10.3 No BGP4+ Routing Information Exists

Isolate the problem according to the failure analysis method listed below if BGP4+ route information does not exist in the displayed route information acquired by this system.

Table 3-37: BGP4+ Failure Analysis Method

No.	Troubleshooting Steps and Command	Action
1	Check the BGP4+ peer status. <code>show ipv6 bgp neighbors</code>	Go to No. 2 if the peer status is other than Established.
		Go to No. 3 if the peer status is Established.
2	Check to see if the BGP4+ setting is correct in configuration.	Go to No. 3 if the configuration is correct.
		Correct the configuration if it is not correct.
3	Check to see if the BGP4+ route is learned. <code>show ipv6 bgp received-routes</code>	Go to No. 4 if the route exist but it is not in active status.
		Go to No.5 if no route exist.
4	Check to see if routing information for the next hop address resolution in BGP4+ exist. <code>show ipv6 route</code>	Go to No.5 if the route information for the next hop address resolution exists.
		When no routing information for the next hop address resolution exist, perform the protocol failure analysis to learn the routing information.
5	Confirm that the routing are not filtered by referring to the configuration.	Check to see if the neighboring router advertises the BGP4+ route.
		Correct the configuration if it is not correct.

3.11 IPv6 Multicast Routing Communication Failure

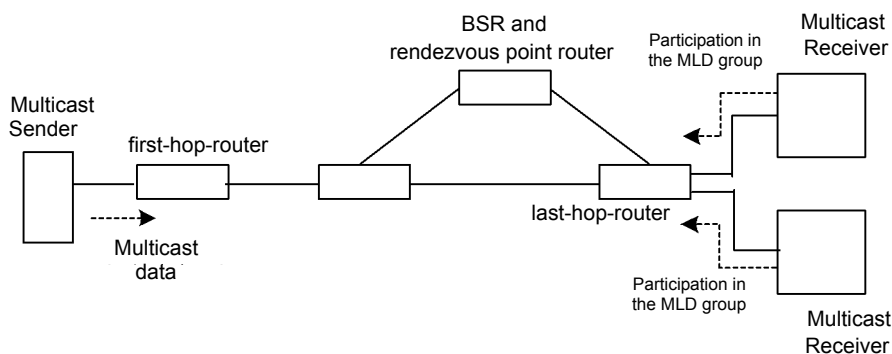
Actions to be taken if IPv6 multicast communication failures occur on this system are described below.

3.11.1 Communication on IPv6 PIM-SM Network Is Disabled

If multicast relay on the IPv6 PIM-SM network configuration is disabled, isolate the cause according to the failure analysis method below.

The figure below illustrates a network example of IPv6 PIM-SM.

Figure 3-16: Example of IPv6 PIM-SM Network



Note

- BSR: This router delivers rendezvous point information (for details, see the manual "Configuration Settings").
- Rendezvous point router: This router relays the packets, for which the relay destination is not determined, toward the multicast receiver (for details, see the manual "Configuration Settings").
- first-hop-router: This router is directly connected to the multicast sender.
- last-hop-router: This router is directly connected to the multicast receiver.

(1) Common check items

The table below shows the common check items for all system in the IPv6 PIM-SM network configuration.

Table 3-38: Common Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that the use of multicast function is designated (ipv6 multicast routing) in the configuration. <code>show running-config</code>	If the use of multicast function is not designated, correct the configuration.
2	Confirm that the address of the loopback interface is set in the configuration. <code>show running-config</code>	If the address of the loopback interface is not set, correct the configuration.
3	Confirm that PIM is running on one or more interfaces. <code>show ipv6 pim interface</code>	If PIM is not running, check the configuration. Set PIM to run on one or more interfaces.
4	Confirm that MLD snooping is set to the interface with PIM enabled. <code>show mld-snooping</code>	When MLD snooping is set, confirm the following: <ul style="list-style-type: none"> • Confirm that multicast router port for MLD snooping is set to the port to which neighboring router connects. • See "3.5.5 Multicast Relay by MLD snooping Is Disabled."

3. Troubleshooting Functional Failures in Operation

No.	Troubleshooting Steps and Command	Action
5	Confirm in the configuration that suppression of protocol packet and multicast packet relay through filtering, etc. is not provided on the interface that allows PIM and MLD to run. <code>show running-config</code>	If suppression of protocol packet and multicast packet relay is provided, correct the configuration.
6	Check the PIM neighboring information. <code>show ipv6 pim neighbor</code>	If the neighboring router is not displayed, check the following: <ul style="list-style-type: none"> • Confirm that PIM is running on the interface connected to the neighboring router using the <code>show ipv6 pim</code> command with "interface" parameter specified. • Verify the settings of the neighboring router.
7	Check to see if the unicast route to the multicast data sender exists. <code>show ipv6 route</code>	If the unicast route does not exist, see " 3.10 IPv6 Unicast Routing Communication Failure. "
8	Confirm that PIM is running on the interface to the next hop address for the multicast data sender. <code>show ipv6 pim interface</code>	If PIM is not running, check the configuration. Set PIM to run on the interface connected to the next hop address for the multicast data sender.
9	Confirm that the PIM-SSM group addresses do not contain the relay target group address, referring to the configuration. <code>show running-config</code>	If the PIM-SSM group addresses contain the relay target group address, correct the configuration.
10	Confirm that BSR is determined. However, this confirmation is not required if the rendezvous point for the relay target group address is a static rendezvous point. <code>show ipv6 pim bsr</code>	If BSR is not determined, check to see if the unicast route to BSR exists. If the unicast route does not exist, see " 3.10 IPv6 Unicast Routing Communication Failure. " If the unicast route exists, check the BSR setting. If the BSR is this system, see " (2)BSR check items. "
11	Confirm that the rendezvous point is determined. <code>show ipv6 pim rp-mapping</code>	If the rendezvous point is not determined, check to see if the unicast route to the rendezvous point exists. If the unicast route does not exist, see " 3.10 IPv6 Unicast Routing Communication Failure. " If the unicast route exists, check the rendezvous point setting. If the rendezvous point is this system, see " (3)Rendezvous point router check items. "
12	Confirm that the rendezvous point group addresses contain the relay target group address. <code>show ipv6 pim rp-mapping</code>	If the relay target group address is not contained, check the rendezvous point setting.
13	Confirm that the multicast relay entry exists. <code>show ipv6 mcache</code>	If the multicast relay entry does not exist, confirm that multicast data has arrived at the upstream port. If multicast data has not arrived, check the setting of the multicast sender or upstream router.
14	Confirm that the multicast routing information exists. <code>show ipv6 mroute</code>	If the multicast routing information does not exist, check the setting of the downstream router.
15	Confirm that multicast routing information or multicast forwarding entry does not exceed the upper limit. Multicast routing information: <code>show ip mroute</code> Multicast forwarding entry: <code>show ip mcache</code> <code>netstat multicast</code>	When warning is output, confirm that unexpected multicast routing information or unexpected multicast forwarding entry has not been created. If much of the negative cache exists in multicast forwarding entry, check to see if no terminal transmitting unnecessary packets exist.

(2) BSR check items

The table below shows the items to be checked when this system is BSR in the IPv6 PIM-SM network configuration.

Table 3-39: BSR Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that this system is a candidate for BSR. <code>show ipv6 pim bsr</code>	If this system is not a candidate for BSR, check the configuration and set the configuration to run this system as a candidate for BSR. Since this system does not run as a candidate for BSR if no address is set for the loopback interface, confirm that an address is set for the loopback interface.
2	Confirm that this system is BSR. <code>show ipv6 pim bsr</code>	If this system is not BSR, check the priority of other BSR candidates. The larger the value, the higher the priority. If the same priority is provided, the BSR candidate with the largest BSR address becomes BSR.

(3) Rendezvous point router check items

The table below shows the items to be checked when this system is the rendezvous point router in the IPv6 PIM-SM network configuration.

Table 3-40: Rendezvous Point Router Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that this system is a candidate of rendezvous point for the relay target group address. <code>show ipv6 pim rp-mapping</code>	If this system is not a candidate of rendezvous point for the relay target group address, check the configuration and set the configuration to run this system as a candidate of rendezvous point for the relay target group address. Since this system does not run as a candidate of rendezvous point if no address is set for the loopback interface, confirm that an address is set for the loopback interface.
2	Confirm that this system is the rendezvous point for the relay target group address. <code>show ipv6 pim rp-hash <Group Address></code>	If this system is not the rendezvous point, check the priority of other candidates of rendezvous point. The smaller the value, the higher the priority. If the priority of another candidate of rendezvous point is higher, this system does not run as the rendezvous point. If the same priority is provided, the rendezvous point is distributed for each group address according to the protocol specifications and this system may not run as the rendezvous point. To run this system preferentially as the rendezvous point, set the priority higher than those of other rendezvous point candidates.

(4) last-hop-router check items

The table below shows the items to be checked when this system is the last-hop-router in the IPv6 PIM-SM network configuration.

Table 3-41: last-hop-router Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that MLD is running on the interface connected to the multicast receiver. <code>show ipv6 mld interface</code>	If MLD is not running, check the configuration and set the configuration to run MLD.
2	Confirm that the multicast receiver participates in the relay target group via MLD. <code>show ipv6 mld group</code>	If the multicast receiver does not participate in the relay target group, check the setting of the multicast receiver.
3	participates and PIM is running, confirm that this system is DR. <code>show ipv6 pim interface</code>	If this system is not DR, check DR of the relay target interface.

No.	Troubleshooting Steps and Command	Action
4	Confirm that MLD snooping is set to the interface with PIM enabled. <code>show mld-snooping</code>	When MLD snooping is set, confirm the following: <ul style="list-style-type: none"> • Confirm that multicast router port for MLD snooping is set to the forwarding port. • See "3.5.5 Multicast Relay by MLD snooping Is Disabled."
5	Confirm that no interface in abnormal state is detected. <code>show ipv6 mld interface</code>	See notices and confirm that warning information is not output. When warning information is output, check the following: <ul style="list-style-type: none"> • L: The number of join request exceeded expected maximum number. Check to see the number of connected users. • Q: The MLD version of neighboring router is different. Adjust it to the MLD version. • R: A user who transmitted reports unreceivable at the present settings exists. Change the MLD version of this system or confirm the setting of the participant. • S: Some of the participant information are being discarded because the number of source exceeded the upper limit defined to store source per message in MLDv2. Check the settings of the participant.

(5) first-hop-router check items

The table below shows the items to be checked when this system is the first-hop-router in the IPv6 PIM-SM network configuration.

Table 3-42: first-hop-router Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that this system is directly connected to the multicast sender.	If not, check the network configuration.
2	Confirm that PIM or MLD is running on the interface connected to the multicast sender. <code>show ipv6 pim interface</code> <code>show ipv6 mld interface</code>	If not running, check the configuration and set the configuration to run PIM or MLD.
3	Confirm that the multicast relay routing information exists. <code>show ipv6 mroute</code>	If the multicast routing information does not exist, confirm that multicast data source address is the network address of the interface directly connected to the multicast sender.

3.11.2 Multicast Data Is Double-relayed on IPv6 PIM-SM Network

If multicast data is double-relayed in the IPv6 PIM-SM network configuration, check the settings of each router and set the configuration to run PIM on the interface for a network having multiple routers.

If double-relay still continues, check the following:

Table 3-43: Check Items When Double-relay Continues

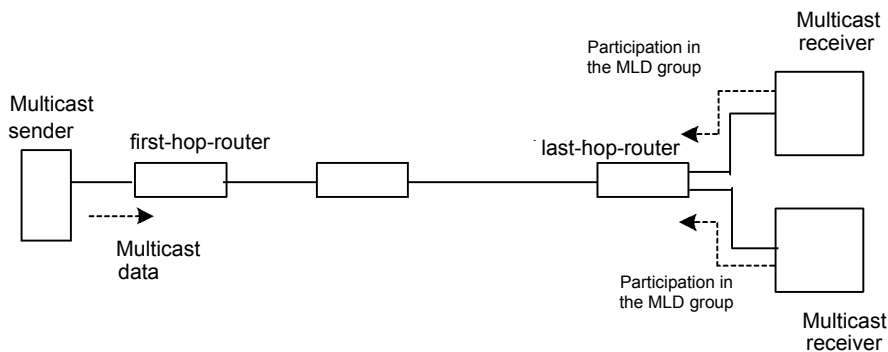
No.	Troubleshooting Steps and Command	Action
1	Check the PIM neighboring information on the interface of the network having multiple routers. <code>show ipv6 pim neighbor</code>	If the neighboring router is not displayed, check the following: <ul style="list-style-type: none"> • Confirm that PIM is running on the interface connected to the neighboring router using the <code>show ipv6 pim</code> command with "interface" parameter specified. • Confirm in the configuration that suppression of protocol packet relay by filtering, etc. is not provided. • Verify the settings of the neighboring router.

3.11.3 Communication on IPv6 PIM-SSM Network Is Disabled

If multicast relay on the IPv6 PIM-SSM network configuration is disabled, isolate the cause according to the failure analysis method below.

The figure below illustrates a network example of IPv6 PIM-SSM.

Figure 3-17: Example of IPv6 PIM-SSM Network



Note

- first-hop-router: This router is directly connected to the multicast sender.
- last-hop-router: This router is directly connected to the multicast receiver.

(1) Common check items

The table below shows the common check items for all system in the IPv6 PIM-SSM network configuration.

Table 3-44: Common Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that the use of multicast function is designated (ipv6 multicast routing) in the configuration. <code>show running-config</code>	If the use of multicast function is not designated, correct the configuration.
2	Confirm that the address of the loopback interface is set in the configuration. <code>show running-config</code>	If the address of the loopback interface is not set, correct the configuration.
3	Confirm that PIM is running on one or more interfaces. <code>show ipv6 pim interface</code>	If PIM is not running, check the configuration. Set PIM to run on one or more interfaces.
4	Confirm that MLD snooping is set to the interface with PIM enabled. <code>show mld-snooping</code>	When MLD snooping is set, confirm the following: <ul style="list-style-type: none"> • Confirm that multicast router port for MLD snooping is set to the ports to which neighboring routers connect. • See "3.5.5 Multicast Relay by MLD snooping Is Disabled."
5	Confirm in the configuration that suppression of protocol packet and multicast packet relay through filtering, etc. is not provided on the interface that allows PIM and MLD to run. <code>show running-config</code>	If suppression of protocol packet and multicast packet relay is provided, correct the configuration.
6	Check the PIM neighboring information. <code>show ipv6 pim neighbor</code>	If the neighboring router is not displayed, check the following: <ul style="list-style-type: none"> • Confirm that PIM is running on the interface connected to the neighboring router using the <code>show ipv6 pim</code> command with "interface" parameter specified. • Verify the settings of the neighboring router.

3. Troubleshooting Functional Failures in Operation

No.	Troubleshooting Steps and Command	Action
7	Check to see if the unicast route to the multicast data sender exists. <code>show ipv6 route</code>	If the unicast route does not exist, see " 3.10 IPv6 Unicast Routing Communication Failure. "
8	Confirm that PIM is running on the sending interface for the unicast route to the multicast data sender. <code>show ipv6 pim interface</code>	If IGMP is not running, check the configuration and set the configuration to run PIM on the sending interface for the unicast route.
9	Confirm that the PIM-SSM group addresses contain the relay target group address, referring to the configuration. <code>show running-config</code>	If the PIM-SSM group addresses do not contain the relay target group address, correct the configuration.
10	Confirm that the multicast relay routing information exists. <code>show ipv6 mroute</code>	If the multicast routing information does not exist, check the setting of the downstream router.
11	Confirm that multicast routing information or multicast forwarding entry does not exceed the upper limit. Multicast routing information: <code>show ipv6 mroute</code> Multicast forwarding entry: <code>show ipv6 mcache</code> <code>netstat multicast</code>	When warning is output, confirm that unexpected multicast routing information or unexpected multicast forwarding entry has not been created. If much of the negative cache exists in multicast forwarding entry, check to see if no terminal transmitting unnecessary packets exist.

(2) last-hop-router check items

The table below shows the items to be checked when this system is the last-hop-router in the IPv6 PIM-SSM network configuration.

Table 3-45: last-hop-router Check Items

No.	Troubleshooting Steps and Command	Action
1	If the mode of multicast receiver is MLDv1/MLDv2 (EXCLUDE mode), confirm in the configuration that the use of PIM-SSM in MLDv1/MLDv2 (EXCLUDE mode) is designated (<code>ipv6 mld ssm-map enable</code>). <code>show running-config</code>	If the use of PIM-SSM in MLDv1/MLDv2 (EXCLUDE mode) is not designated, correct the configuration.
2	If the mode of multicast receiver is MLDv1/MLDv2 (EXCLUDE mode), confirm in the configuration that cooperation with PIM-SSM in MLDv1/MLDv2 (EXCLUDE mode) is set for the group address and source address to be relayed by PIM-SSM (<code>ipv6 mld ssm-map static</code>). <code>show running-config</code>	If cooperation with PIM-SSM in MLDv1/MLDv2 (EXCLUDE mode) is not designated, correct the configuration.
3	Confirm that MLD is running on the interface connected to the multicast receiver. <code>show ipv6 mld interface</code>	If MLD is not running, check the configuration and set the configuration to run MLD.
4	Confirm that MLD warning information is not displayed on the interface connected to the multicast receiver. <code>show ipv6 mld interface</code>	If displayed, take the action against the warning. For details on the warning, see "Operation Commands."
5	Confirm that the multicast receiver participates in the relay target group via MLD. <code>show ipv6 mld group</code>	If the group does not participate in the relay target group, check the setting of the multicast receiver.
6	Confirm that the source address is registered in the MLD group information. <code>show ipv6 mld group</code>	If the mode of multicast receiver is MLDv2 (INCLUDE mode) and the source address is not registered, check the multicast receiver. If the mode of multicast receiver is MLDv1/MLDv2 (EXCLUDE mode), confirm in the configuration that cooperation with PIM-SSM is set.
7	If there is an interface in which the relay target group participates and PIM is running, confirm that this system is DR. <code>show ipv6 pim interface</code>	If this system is not DR, check DR of the relay target interface.

No.	Troubleshooting Steps and Command	Action
8	Check to see if IGMP snooping is set to the port in which static group join function is running. <code>show mld-snooping</code>	When MLD snooping is set, confirm the following: <ul style="list-style-type: none"> • Chec to see if the forwarding port is set as a multicast port for MLD snooping • See "3.5.5 Multicast Relay by MLD snooping Is Disabled."
9	Confirm that no interface in abnormal state is detected. <code>show ipv6 mld interface</code>	See notices and confirm that warning information is not output. When warning information is output, check the following: <ul style="list-style-type: none"> • L: The number of join request exceeded expected maximum number. Check to see the number of connected users. • Q: The MLD version of neighboring router is different. Adjust it to the MLD version. • R: A user who transmitted reports unreceivable at the present settings exists. Change the MLD version of this system or confirm the setting of the participant. • S: Some of the participant information are being discarded because the number of source exceeded the upper limit defined to store source per message in MLDv2. Check the settings of the participant.

(3) first-hop-router check items

The table below shows the items to be checked when this system is the first-hop-router in the IPv6 PIM-SSM network configuration.

Table 3-46: first-hop-router Check Items

No.	Troubleshooting Steps and Command	Action
1	Confirm that this system is directly connected to the multicast sender.	If not, check the network configuration.
2	Confirm that PIM or MLD is running on the interface connected to the multicast sender. <code>show ipv6 pim interface</code> <code>show ipv6 mld interface</code>	If not running, check the configuration and set the configuration to run PIM or MLD.
3	Check to see if multicast data arrives at this system.	If multicast data has not arrived, check the setting of the multicast sender.
4	Check to see if the group address and source address in multicast data match those in the multicast routing information. <code>show ipv6 mroute</code> <code>show netstat multicast</code>	If the group address and source address do not match, check the settings of the multicast sender and last-hop-router.

3.11.4 Multicast Data Is Double-relayed on IPv6 PIM-SSM Network

If multicast data is double-relayed in the IPv6 PIM-SSM network configuration, check the settings of each router and set the configuration to run PIM on the interface for a network having multiple routers.

If double-relay still continues, check the following:

3. Troubleshooting Functional Failures in Operation

Table 3-47: Check Items When Double-relay Continues

No.	Troubleshooting Steps and Command	Action
1	Check the PIM neighboring information on the interface of the network having multiple routers. <code>show ipv6 pim neighbor</code>	If the neighboring router is not displayed, check the following: <ul style="list-style-type: none">• Confirm that PIM is running on the interface connected to the neighboring router using the <code>show ipv6 pim</code> command with "interface" parameter specified.• Confirm in the configuration that suppression of protocol packet relay by filtering, etc. is not provided.• Verify the settings of the neighboring router.

3.12 Layer 2 Authentication Communication Failure

3.12.1 Communication Failure on Using IEEE 802.1X

If authentication is disabled when using IEEE 802.1X, isolate the problem by following failure analysis methods shown in the table below.

Table 3-48: IEEE 802.1X Failure Analysis Method

No.	Troubleshooting Steps and Command	Action
1	Execute the <code>show dot1x</code> command and check the operation status of the IEEE802.1X.	If "Dot1x doesn't seem to be running" is displayed, IEEE802.1X has stopped. Check to see if the <code>dot1x system-auth-control</code> command is set in the configuration. Go to No. 2 if "System 802.1X: Enable" is displayed.
2	Execute the <code>show dot1x statistics</code> command and confirm that EAPOL is exchanged.	If RxTotal of [EAPOL frames] is 0, the terminal does not send EAPOL. If RxInvalid or RxLenErr is not 0, illegal EAPOL has been received from the terminal. When illegal EAPOL is received, log is recorded. The log can be browsed using <code>show dot1x logging</code> command. The log shows the "Invalid EAPOL frame received" message and the contents of illegal EAPOL. Check the Supplicant setting on the terminal. Otherwise, go to No. 3.
3	Execute the <code>show dot1x statistics</code> command and confirm that data is sent to the RADIUS server.	If "TxTotal" of [EAP overRADIUS frames] is set to 0, it indicates that no data is sent to the RADIUS server. Confirm the following: <ul style="list-style-type: none"> • Check to see if <code>aaa authentication dot1x default group radius</code> is set by the configuration command. • Check to see if the configuration command <code>radius-server host</code> is set correctly. • If the authentication mode is port authentication or VLAN authentication (static), confirm that the authentication terminal is not registered by the configuration command <code>mac-address-table static</code>. If the authentication mode is VLAN authentication (dynamic), confirm that the authentication terminal is not registered by the configuration command <code>mac-address</code>. • If the authentication mode is VLAN authentication (dynamic), check to see if <code>aaa authorization network default group radius</code> is set by the configuration command. Otherwise, go to No. 4.
4	Execute the <code>show dot1x statistics</code> command and confirm that data is received from the RADIUS server.	If "RxTotal" of [EAP overRADIUS frames] is set to 0, packets are not received from the RADIUS server. Confirm the following: <ul style="list-style-type: none"> • If the RADIUS server is accommodated in the remote network, confirm that the route to the remote network exists. • Confirm that the port of the RADIUS server is excluded from authentication. Otherwise, go to No. 5.
5	Execute the <code>show dot1x logging</code> command and check exchange with the RADIUS server.	<ul style="list-style-type: none"> • If "Invalid EAP over RADIUS frames received" is output, illegal packets are received from the RADIUS server. Check to see if the RADIUS server is normally operating. • If "Failed to connect to RADIUS server" is output, connection to the RADIUS server failed. Check to see if the RADIUS server is normally operating. Otherwise, go to No. 6.

3. Troubleshooting Functional Failures in Operation

No.	Troubleshooting Steps and Command	Action
6	Execute the <code>show dot1x logging</code> command and check to see if authentication failed.	<ul style="list-style-type: none"> • If "New Supplicant Auth Fail." is output, authentication failed due to the following cause. Check to see if there is any problem. <ul style="list-style-type: none"> (1) User ID or password is not registered on the authentication server. (2) User ID or password input error • If "The number of supplicants on the switch is full" is output, authentication failed because the maximum number of supplicants for the system was exceeded. • If "The number of supplicants on the interfaces is full" is output, authentication failed because the maximum number of supplicants on the interface was exceeded. • If "Failed to authenticate the supplicant because it could not be registered to mac-address-table." is output, authentication was successful but MAC address table setting for hardware failed. See the corresponding part in manual "Message Log Reference" and follow [Action] described. • If "Failed to authenticate the supplicant because it could not be registered to MAC VLAN." is output, authentication was successful but H/W MAC VLAN table setting failed. See the corresponding part in manual "Message Log Reference" and follow [Action] described. For IP8800/S6700, IP8800/S6600, and IP8800/S6700, see "4.2.2 Action to Be Taken When VLAN Identification Table Resource Shortage Occurs" <p>If the above is not applicable and the authentication target port is VLAN authentication (dynamic) mode, go to No. 7. For other authentication unit modes, see the log of the RADIUS server and check to see if authentication failed.</p>

No.	Troubleshooting Steps and Command	Action
7	Execute the <code>show dot1x logging</code> command and check to see if dynamic assignment of VLAN authentication (dynamic) failed.	<ul style="list-style-type: none"> • If "Failed to assign VLAN.(Reason: No Tunnel-Type Attribute)" is output, the dynamic assignment has been failed as there is no Tunnel-Type attribute in the RADIUS attribute of the RADIUS frame. Add the Tunnel-Type attribute in setting of the RADIUS attribute for the RADIUS server. • If "Failed to assign VLAN.(Reason:Tunnel-Type Attribute is not VLAN(13))" is output, the dynamic assignment has been failed as the value of Tunnel-Type attribute of the RADIUS attribute is not VLAN(13). Set the value of Tunnel-Type for the RADIUS server to VLAN(13). • If "Failed to assign VLAN.(Reason: No Tunnel-Medium-Type Attribute)" is output, the dynamic assignment has been failed as there is no Tunnel-Medium-Type attribute of RADIUS server. Add the Tunnel-Medium-Type attribute in setting of the RADIUS attribute for the RADIUS server. • If "Failed to assign VLAN. (Reason: Tunnel-Medium-Type Attribute is not IEEE802(6))" is output, the dynamic assignment has been failed as the value of Tunnel-Medium-Type attribute is not IEEE802(6) or the Tag value did not match with the Tag of the Tunnel-Type attribute although the Tunnel-Medium-Type value was matched. Set the Tunnel-Medium-Type attribute value of the RADIUS attribute for the RADIUS server or Tag to the correct value. • If "Failed to assign VLAN.(Reason: No Tunnel-Private-Group-ID Attribute)" is output, the dynamic assignment has been failed as Tunnel-Private-Group-ID attribute of the RADIUS attribute for the RADIUS server is not set. Set the Tunnel-Private-Group-ID attribute of the RADIUS attribute for the RADIUS server. • If "Failed to assign VLAN.(Reason: Invalid Tunnel-Private-Group-ID Attribute)" is output, the dynamic assignment has been failed as Tunnel-Private-Group-ID attribute of the RADIUS attribute contained an illegal value. Set the correct VLAN ID for the Tunnel-Private-Group-ID attribute of the RADIUS attribute for the RADIUS server. • If "Failed to assign VLAN. (Reason: The VLAN ID is out of range.)" is output, the dynamic assignment has been failed as VLAN ID set for the Tunnel-Private-Group-ID attribute of the RADIUS attribute for the RADIUS server was out of range. Set the correct VLAN ID for the Tunnel-Private-Group-ID attribute. • If "Failed to assign VLAN. (Reason: The port doesn't belong to VLAN.)" is output, the dynamic assignment has been failed as authentication port does not belong to the VLAN ID specified for the Tunnel-Private-Group-ID attribute of the RADIUS attribute for the RADIUS server. Match the VLAN ID set for the Tunnel-Private-Group-ID attribute of the RADIUS attribute for the RADIUS server with the VLAN ID of MAC VLAN set on the authentication port. • If "Failed to assign VLAN. (Reason: The VLAN ID is not set to radius-vlan.)" is output, the VLAN ID specified for the Tunnel-Private-Group-ID attribute as the RADIUS attribute for the RADIUS server was not the target for VLAN authentication (dynamic). Match the VLAN ID set for the Tunnel-Private-Group-ID attribute of the RADIUS attribute for the RADIUS server with the VLAN ID of MAC VLAN set on the authentication port. <p>Otherwise, see the log of the RADIUS server and check to see if authentication failed.</p>

If communication is not possible on the port or VLAN on which IEEE 802.1X runs, isolate the problem by following failure analysis methods shown in the table below. Otherwise, see "[3.5 Layer 2 Network Communication Failure.](#)" **[IP8800/S3600] [IP8800/S2400]**

Table 3-49: IEEE 802.1X Failure Analysis Method [IP8800/S3600] [IP8800/S2400]

No.	Troubleshooting Steps and Command	Action
1	Confirm that VLAN with VLAN authentication (static) set and other VLANs are not provided on the trunk port.	Since communication is enabled only with the VLAN on which VLAN authentication (static) is set, exclude the port from authentication or set the VLAN with VLAN authentication (static) and other VLANs on different ports.
2	Check to see if the authenticated terminal has moved to the non-authentication port in the same VLAN.	If the terminal authenticated on this system moves to the non-authentication port, communication is disabled unless authentication information is released. Execute the <code>clear dot1x auth-state</code> command to release the authenticated state on the target terminal.

3.12.2 Communication Failure on Using Web Authentication

Isolate the problem according to the failure analysis method described in "[Table 3-50: Failure Analysis Method for Web Authentication](#)."

For checking Web authentication configuration and accounting information, isolate the problem according to the failure analysis method described in "[Table 3-51: Checking Web Authentication Configuration](#)" and "[Table 3-52: Web Authentication Failure Analysis Method](#)" each.

Table 3-50: Failure Analysis Method for Web Authentication

No.	Troubleshooting Steps and Command	Action
1	Check to see if the login screen is displayed on the terminal.	<ul style="list-style-type: none"> • If login and logout screens are not displayed, go to No. 2. • If login screen is displayed in the case of local authentication method, go to No.3. • If login screen is displayed in the case of RADIUS authentication method, go to No.7. • If operation log message appears, go to No.14.
2	Check to see if login and logout URLs are correct.	<ul style="list-style-type: none"> • If not correct, use correct URLs. • In static VLAN mode, if login screen and logout screen are unable to display, check the following and correct them if necessary: <ul style="list-style-type: none"> - Check to see if IP address dedicated for Web authentication is configured by configuration command <code>web-authentication ip address</code> or URL redirect is enabled by configuration command <code>web-authentication redirect enable</code>. - When URL redirect is enabled in IP8800/S3600 or IP8800/S2400 models, check to see if IP address dedicated for Web authentication is configured by configuration command <code>web-authentication ip address</code>. - For IP8800/S6700, IP8800/S6600, and IP8800/S6300 models, check to see if IP address dedicated for Web authentication is configured by configuration command <code>web-authentication ip address</code>. • Otherwise, go to No. 3.
3	Check to see if Web server is working.	<ul style="list-style-type: none"> • Execute the following command and confirm that Web server is working properly. If Web server is working, go to No.4. [Command] <code># ps -aux grep httpd</code> [Confirmation] If <code>/usr/local/sbin/httpd</code> is displayed by entering the <code>ps</code> command, it indicates Web server is working properly. • If Web server is not working properly, check the status by using the configuration command <code>web-authentication web-port</code>.

No.	Troubleshooting Steps and Command	Action
4	Check to see authentication Ipv4 access list	<ul style="list-style-type: none"> • For IP8800/S6700, IP8800/S6600, and IP8800/S6300 models, go to No.9. • If a terminal before authentication sends packets out of the system, confirm that authentication IPv4 access list is applied. If access list and authentication IPv4 access list both are applied to the port for authentication, make sure the filter conditions described in IPv4 access list are set in the access list as well. • Confirm that filter condition for denying packets (such as deny ip) is not set to the access list/authentication IPv4 access list applied to the port for authentication. • Confirm that the IP address dedicated for Web authentication is not set in the filter condition of authentication IPv4 access list. • Confirm that "any" is not specified as a destination address in the filter conditions of authentication IPv4 access list. • Otherwise, go to No.9.
5	Use the <code>show web-authentication user</code> command to check to see if user ID is registered.	<ul style="list-style-type: none"> • If not registered, use the <code>set web-authentication user</code> command to register the user ID, password, and VLAN-ID. • Otherwise, go to No. 6.
6	Check to see if the entered password is correct.	<ul style="list-style-type: none"> • If not correct, use the <code>set web-authentication passwd</code> command to change the password, or use the <code>remove web-authentication user</code> command to delete the user ID once, then use the <code>set web-authentication user</code> command to register the user ID, password, and VLAN-ID again. • Otherwise, go to No. 9.
7	Use the <code>show web-authentication statistics</code> command to check the communication status with the RADIUS server.	<ul style="list-style-type: none"> • If the value of "TxError" of "[RADIUS frames]" is "0", check to see if <code>aaa authentication web-authentication default group radius and radius-server host</code> in the configuration command are set correctly. • For IP8800/S3600 and IP8800/S2400 models, even though the dead interval lets RADIUS server get recovered from no-response state and become able to communicate, the system is not able to collate with the RADIUS server during a period of time specified by the configuration command <code>authentication radius-server dead-interval</code>. As a result, authentication error occurs. In this case, if the period of time is too long for the system to wait for an authentication error response, change the set value of configuration command <code>authentication radius-server dead-interval</code> or execute the <code>clear web-authentication dead-interval-timer</code> command. Authentication action against the first RADIUS will be taken again. • Otherwise, go to No. 8.
8	Check to see if the user ID and password are registered for the RADIUS server.	<ul style="list-style-type: none"> • If not registered, register the user ID and password for the RADIUS server. • Otherwise, go to No. 9.
9	Use the <code>show web-authentication statistics</code> command to check to see if Web authentication statistical information is displayed.	<ul style="list-style-type: none"> • If not displayed, go to No. 8. • Otherwise, go to No. 11.
10	Check to see if configuration command <code>web-authentication system-auth-control</code> is set.	<ul style="list-style-type: none"> • If not, set the configuration command <code>web-authentication system-auth-control</code>. • Otherwise, go to No. 11.

3. Troubleshooting Functional Failures in Operation

No.	Troubleshooting Steps and Command	Action
11	Execute the <code>show web-authentication logging</code> command to check to see if the system operates correctly.	<ul style="list-style-type: none"> • If the log "The login failed because of hardware restriction." is output by the <code>show web-authentication logging</code> command, see "4.2.2 Action to Be Taken When VLAN Identification Table Resource Shortage Occurs." • In static VLAN mode, if authentication information of the port to which the terminal connects is not displayed, check to see if data on the port for authentication is correctly set by using the configuration command <code>web-authentication port</code>. In addition, make sure the status of the authentication port is neither linkdown nor shutdown. • Otherwise, go to No.13.
12	If no account is recorded in the accounting server, use the <code>show web-authentication statistics</code> command to check the communication status with the accounting server.	<ul style="list-style-type: none"> • If the value of "TxError" of "[Account frames]" is "0", check to see if <code>aaa accounting web-authentication default start-stop group radius and radius-server host</code> in the configuration command are set correctly. • Otherwise, check Web authentication configuration.
13	Check to see if all the terminals are not able to be authenticated.	<ul style="list-style-type: none"> • When all the target terminal are unable to be authenticated, restart the Web server by using the <code>restart web-authentication web-server</code> command. • Otherwise, check to see the configuration of the Web authentication and correct it if necessary.
14	Check to see the operation log by using the <code>show logging</code> command.	<ul style="list-style-type: none"> • When you perform the following operations, Web server (httpd) stop and restart messages might appear as operation logs. <ol style="list-style-type: none"> (1) When Web authentication is activated by the <code>web-authentication system-auth-control</code> command soon after suspended by the <code>no web-authentication system-auth-control</code> command (2) When the system changeover in IP8800/S6700(BCU), IP8800/S6600(CSU), or IP8800/S6300(MSU) occurs (3) When Web server is restarted by using the <code>restart web-authentication web-server</code> command <pre>[Web server (httpd) stop message] Level: E7 Message Identification:2a001000 Message: httpd aborted. [Web server (httpd) restart message] Level: R7 Message Identification:2a001000 Message: httpd restarted.</pre> <p>The messages above indicate Web server is automatically stopped and restarted. The Web server starts to perform authentication actions after restarted.</p> • Otherwise, see the manual "Message Log Reference."

For the configuration relating to the Web authentication, check the following:

Table 3-51: Checking Web Authentication Configuration

No.	Check Point	Troubleshooting Steps
1	Setting of Web authentication configuration	<p>Confirm that the following configuration commands are set correctly:</p> <p><common setting></p> <ul style="list-style-type: none"> • <code>aaa accounting web-authentication default start-stop group radius</code> • <code>aaa authentication web-authentication default group radius</code> • <code>web-authentication system-auth-control</code> <p><when dynamic vlan mode is set></p> <ul style="list-style-type: none"> • <code>web-authentication auto-logout</code> • <code>web-authentication max-timer</code> • <code>web-authentication max-user</code> • <code>web-authentication vlan</code> <p><when static vlan mode is set></p> <ul style="list-style-type: none"> • <code>web-authentication ip address</code> • <code>web-authentication port</code> • <code>web-authentication static-vlan max-user</code> • <code>web-authentication web-port</code> <p>When you use IP8800/S3600 or IP8800/S2400, confirm the settings by using the following commands.</p> <ul style="list-style-type: none"> • <code>authentication arp-relay</code> • <code>authentication ip access-group</code> • <code>web-authentication redirect enable</code> • <code>web-authentication redirect-mode</code>
2	IP address setting for VLAN interface	<p>Using dynamic vlan mode, confirm that the IP address is correctly set to each VLAN interface:</p> <ul style="list-style-type: none"> • Pre-authentication VLAN • Post-authentication
3	Setting of DHCP relay agent	<p>When using the external DHCP server and L3 switches in dynamic vlan mode, check that DHCP relay agent between the following VLANs is set correctly.</p> <ul style="list-style-type: none"> • Between pre-authentication VLAN and server VLAN • Between post-authentication VLAN and server VLAN
4	Filter setting	<p>When using L3 switches in dynamic vlan mode, confirm that the following inter-VLAN filter is set correctly.</p> <ul style="list-style-type: none"> • Between pre-authentication VLAN and post-authentication VLAN: Set the filter to disable all IP communications. • Between post-authentication VLAN and pre-authentication VLAN: Set the filter to relay Web browser communication only. <p>Certain packets may have been discarded by filtering, or packets may have been discarded through bandwidth monitoring, discarding control, or shaper of the QoS control.</p> <p>Check to see if the conditions of filtering and QoS control in the configuration have been set up correctly and if bandwidth monitoring, discarding control, or shaper has been set up appropriately for system operation. For the procedure, see "3.23.1 Checking Filtering/QoS Setting Information."</p>

3. Troubleshooting Functional Failures in Operation

No.	Check Point	Troubleshooting Steps
5	Check to see the access filter setting for authentication.	When using IP8800/S3600 or IP8800/S2400 model in static VLAN mode, confirm that the filter condition permits pre-authenticated terminals to send packets out of the system by the configuration command <code>authentication ip access-group</code> or <code>ip access-list extended</code> .
6	Check to see the ARP relay setting.	When using IP8800/S3600 or IP8800/S2400 model in static VLAN mode, confirm that the setting permits pre-authenticated terminals to send packets out of the system by the configuration command <code>authentication arp-relay</code> .

For the configuration relating to the Web authentication accounting, check the following.

Table 3-52: Web Authentication Failure Analysis Method

No.	Troubleshooting Steps and Command	Action
1	Check to see if account has been recorded after authentication.	<ul style="list-style-type: none"> When authentication status is not displayed by the <code>show mac-authentication login</code> command, see "Table 3-50: Failure Analysis Method for Web Authentication." If authentication status is not recorded in the accounting server, go to No.2. If authentication status is not recorded in the syslog server, go to No.3.
2	Check to see communication status with accounting server by the <code>show web-authentication statistics</code> command.	<ul style="list-style-type: none"> When "TxTotal" of [Account frames] indicates 0, check to see if the setting by configuration command <code>aaa accounting web-authentication default start-stop group radius</code> or <code>radius-server host</code> is correct. Otherwise, check the configurations for Web authentication.
3	Check to see the settings of syslog server.	<p>Confirm the settings by the following commands are correct.</p> <ul style="list-style-type: none"> Confirm that syslog server is configured by the <code>logging host</code> command. Confirm that "aut" is set as an event kind by the <code>logging event-kind</code> command. Confirm that the logging is enabled by the <code>web-authentication logging enable</code> command.

3.12.3 Communication Failure on Using MAC Authentication

For MAC authentication failure, isolate the problem according to the failure analysis method described in "[Table 3-53: Failure Analysis Method for MAC Authentication.](#)"

For confirming Web authentication configuration and accounting information, isolate the problem according to the failure analysis method described in "[Table 3-54: Checking MAC Authentication Configuration](#)" and "[Table 3-55: MAC Authentication Failure Analysis Method.](#)"

Table 3-53: Failure Analysis Method for MAC Authentication

No.	Troubleshooting Steps and Command	Action
1	Check to see if the terminal can communicate.	<ul style="list-style-type: none"> • If authentication in Local authentication method failed, go to No. 2. • If authentication in RADIUS authentication method failed, go to No.3. • Otherwise, go to No.5.
2	Check to see if MAC address and VLAN ID are registered by the <code>show mac-authentication mac-address</code> command.	<ul style="list-style-type: none"> • If MAC address is not registered yet, set MAC address and VLAN ID by the <code>set mac-authentication mac-address</code> command. • Otherwise, go to No. 5.
3	Check to see the status of communication with RADIUS server by the <code>show mac-authentication statistics</code> command.	<ul style="list-style-type: none"> • When "TxTotal" of [Account frames] indicates 0, confirm all of the settings by configuration commands (<code>aaa accounting web-authentication default start-stop group radius, radius-server host, and mac-authentication radius-server host</code>) are correct. • For IP8800/S3600 and IP8800/S2400 models, even though the dead interval lets RADIUS server get recovered from no-response state and become able to communicate, the system is not able to collate with the RADIUS server during a period of time specified by configuration command <code>authentication radius-server dead-interval</code>. As a result, an authentication error occurs. In this case, if the period of time is too long for the system to wait for an authentication error response, change the set value of configuration command <code>authentication radius-server dead-interval</code> or execute the <code>clear web-authentication dead-interval-timer</code> command. Authentication action against the first RADIUS will be taken again. • Otherwise, go to No. 4.
4	Check to see if MAC address and password are registered in RADIUS server.	<ul style="list-style-type: none"> • If MAC address has not been registered as a User ID for RADIUS Server yet, register it. • If you use MAC address as a password, set the same value as in MAC address. • Once you registered common values to the RADIUS servers as a password, check to see if the password is the same as one registered by the configuration command <code>mac-authentication password</code>. • Otherwise, go to No.5.

3. Troubleshooting Functional Failures in Operation

No.	Troubleshooting Steps and Command	Action
5	Check to see authentication IPv4 access list.	<ul style="list-style-type: none"> • For IP8800/S6700, IP8800/S6600, and IP8800/S6300 models, go to No.6. • For IP8800/S3600 and IP8800/S2400 models, if pre-authenticated terminal sends packets out of the system, confirm that authentication IPv4 access list is applied. If access list and authentication IPv4 access list both are applied to the port for authentication, make sure the filter conditions described in IPv4 access list are set in the access list as well. • If communication is established without any authentication, confirm that filter condition for permitting packets (such as permit ip any) is not applied to the port for authentication. • Even if the filter condition (deny ip any any) is set to authentication IPv4 access list applied to the port for authentication, MAC authentication is performed using received ARP packets. If you want to put the port out of MAC authentication, you need to disable it by using the configuration command <code>no mac-authentication port</code>. • Otherwise, go to No.6.
6	Check to see if statistics information on MAC authentication is displayed by the <code>show mac-authentication statistics</code> command	<ul style="list-style-type: none"> • If statistics information on MAC authentication is not displayed, go to No.7. • Otherwise, go to No.8.
7	Confirm that the setting is completed by the configuration command <code>mac-authentication system-auth-control</code> .	<ul style="list-style-type: none"> • If the setting is not completed by the configuration command <code>mac-authentication system-auth-control</code>, complete it. • Confirm that the port for authentication is correctly configured by the configuration command <code>mac-authentication port</code>. • Confirm that the port for authentication is neither linkdown nor shutdown. • Otherwise, go to No.8.
8	Confirm that actions caused by the <code>show mac-authentication logging</code> command is completed without any problem.	<ul style="list-style-type: none"> • If terminals have authenticated themselves up to the maximum number of lines, you need to wait until other terminal cancel the authentication. • Otherwise, check to see the configuration of MAC authentication.

For the configuration relating to the MAC authentication, check the following:

Table 3-54: Checking MAC Authentication Configuration

No.	Check Point	Troubleshooting Steps
1	Setting of MAC authentication configuration	<p>Confirm that the settings by the following configuration commands are correct:</p> <ul style="list-style-type: none"> • <code>aaa accounting mac-authentication default start-stop group radius</code> • <code>aaa authentication mac-authentication default group radius</code> • <code>mac-authentication password</code> • <code>mac-authentication port</code> • <code>mac-authentication radius-server host</code> • <code>mac-authentication static-vlan max-user</code> • <code>mac-authentication system-auth-control</code>
5	Access filter setting for authentication	<p>When using IP8800/S3600 or IP8800/S2400 model in static VLAN mode, confirm that the filter condition permits pre-authenticated terminals to send packets out of the system is set by the configuration command <code>authentication ip access-group</code> or <code>ip access-list extended</code>.</p>

For the configuration relating to the MAC authentication accounting, check the following.

Table 3-55: MAC Authentication Failure Analysis Method

No.	Check Point	Troubleshooting Steps
1	Check to see if account has been recorded in the authentication result.	<ul style="list-style-type: none"> • When authentication status is not displayed by the <code>show mac-authentication login</code> command, see "Table 3-53: Failure Analysis Method for MAC Authentication." • If authentication status is not recorded in the accounting server, go to No.2. • If authentication status is not recorded in the syslog server, go to No.3.
2	Check to see communication status with accounting server by the <code>show mac-authentication statistics</code> command.	<ul style="list-style-type: none"> • When "TxTotal" of [Account frames] indicates 0, confirm the setting by configuration command <code>aaa accounting mac-authentication default start-stop group radius, radius-server host, or mac-authentication radius-server host</code> is correct. • Otherwise, check the configurations for MAC authentication.
3	Check to see the settings of syslog server.	<p>Confirm the settings by the following commands are correct.</p> <ul style="list-style-type: none"> • Confirm syslog server is configured by the <code>logging host</code> command • Confirm "aut" is set as an event kind by the <code>logging event-kind</code> command. • Confirm the setting by the <code>mac-authentication logging enable</code> command is done.

3.12.4 Communication Failure on Using Authentication VLAN [OP-VAA]

For failures that occurred when using the authentication VLAN, isolate the cause according to the table below.

3. Troubleshooting Functional Failures in Operation

Table 3-56: Authentication VLAN Failure Analysis Method

No.	Troubleshooting Steps and Command	Action
1	Execute the <code>show logging</code> command and check to see if hardware failures are recorded in the operation log.	<ul style="list-style-type: none"> • If hardware failures are recorded in the operation log, replace the system. • Otherwise, go to No. 2.
2	Execute the <code>show fense server</code> command and confirm that the system runs normally.	<ul style="list-style-type: none"> • If error message "Connection failed to VAA program." is displayed, go to No. 8. • Otherwise, go to No. 3.
3	Execute the <code>show fense server</code> command and check the operation status of the authentication VLAN.	<ul style="list-style-type: none"> • If VAA NAME is not set ("-") displayed), the fense vaa-name configuration is not set. Set the fense vaa-name configuration. • If "disable" is displayed in Status for each <vaa_id>, the authentication VLAN has stopped. Check the configuration. • Otherwise, go to No. 4.
4	Execute the <code>show fense server</code> command and check the status of connection with the authentication server.	<ul style="list-style-type: none"> • If "Server Address" indication for each <vaa_id> is different from the IP address of the authentication server or "Port" indication is different from the TCP port number of the authentication server, communication with the authentication server is disabled. Check the configuration. • If other than CONNECTED is displayed in "Agent Status" for each <vaa_id>, connection with the authentication server is disconnected. Check the authentication server status and settings. • Otherwise, go to No. 5.
5	Specify "detail" parameter by the <code>show fense server</code> command, and check the setting status of the fense vlan configuration.	<ul style="list-style-type: none"> • If VLAN ID for each <vaa_id> is not displayed or the display contents are incorrect, VLAN to be switched over after terminal authentication is not provided. Check the configuration. • Otherwise, go to No. 6.
6	Execute the <code>show fense statistics</code> command a few times and check the status of connection with the authentication server.	<ul style="list-style-type: none"> • If "Connect Failure Count" and "Timeout Disconnect Count" for each <vaa_id> are incremented, connection with the authentication server is unstable. Check the status of network to the authentication server. • If the status of network is normal, check that value "alive-time" set by the configuration command <code>fense alive-timer</code> and the value of parameters set for the authentication server ("HCinterval" and "RecvMsgTimeout") are as follows: $alive-time \geq HCinterval + 5$ $RecvMsgTimeout \geq HCinterval + 5$ • If communication with the authentication server is connected and disconnected repeatedly, use the <code>restart vaa</code> command to restart the authentication VLAN, VLANaccessController at the authentication server, and each function of the authentication VLAN. • Otherwise, go to No. 7.
7	Execute the <code>show fense statistics</code> command and confirm that exchange with the MAC VLAN function is performed.	<ul style="list-style-type: none"> • If each Request count of "VLANaccessAgent Recv Message" displayed for each <vaa_id> does not match each Request count of "Target-VLAN Registration," internal conflict has occurred. Restart the authentication VLAN using the <code>restart vaa</code> command. • Otherwise, go to No. 8.

No.	Troubleshooting Steps and Command	Action
8	Execute the <code>show vlan mac-vlan</code> command and confirm that the authenticated MAC address is registered in the MAC VLAN function.	<ul style="list-style-type: none"> • If the authenticated MAC address is registered by the <code>show vlan mac-vlan</code> command, authentication for the MAC address is not enabled. Clear the MAC address registered by the command. • If the MAC address authenticated for each VLAN is not displayed, internal conflict has occurred. Restart the authentication VLAN using the <code>restart vaa</code> command. • If the authenticated MAC address is not displayed even though the authentication VLAN is restarted, restart the L2MAC manager program using the <code>restart vlan</code> command with "mac-manager" parameter specified. • Otherwise, go to No. 9.
9	Execute the <code>show fense logging</code> command and confirm that exchange with the authentication server is performed.	<ul style="list-style-type: none"> • If the "The registration of the MAC address failed." log is output by the <code>show fense logging</code> command, see "4.2.2 Action to Be Taken When VLAN Identification Table Resource Shortage Occurs." [IP8800/S6700] [IP8800/S6600] [IP8800/S6300] <p>Otherwise, check the configuration of the authentication VLAN.</p>

For the configuration relating to the authentication VLAN, check the following.

Table 3-57: Checking Authentication VLAN Configuration

No.	Check Point	Troubleshooting Steps
1	Setting of authentication VLAN configuration	<p>Confirm that the following configuration command is set correctly:</p> <ul style="list-style-type: none"> • <code>fense vaa-name</code> • <code>fense vlan</code> • <code>fense server</code> • <code>fense retry-count</code> • <code>fense retry-timer</code> • <code>fense alive-timer</code>
2	IP address setting for VLAN interface	<p>Confirm that the IP address is set correctly for each VLAN interface:</p> <ul style="list-style-type: none"> • Pre-authentication VLAN • Post-authentication VLAN • Authentication server VLAN • VLAN to access

3. Troubleshooting Functional Failures in Operation

No.	Check Point	Troubleshooting Steps
3	Setting of DHCP relay agent	<p>Confirm that the following inter-VLAN DHCP relay agent is set correctly:</p> <ul style="list-style-type: none"> • Between pre-authentication VLAN and authentication server VLAN • Between post-authentication VLAN and authentication server VLAN
4	Filter setting	<p>Confirm that the following inter-VLAN filter is set correctly:</p> <ul style="list-style-type: none"> • Between pre-authentication VLAN and post-authentication VLAN: Set the filter to disable all IP communications. • Between pre-authentication VLAN and authentication server VLAN: Set the filter to relay the HTTP, DHCP, and ICMP communications only. • Between pre-authentication VLAN and VLAN to access: Set the filter to disable all IP communications. • Between post-authentication VLAN and authentication server VLAN: Set the filter to relay the HTTP, DHCP, and ICMP communications only. • Between authentication server VLAN and VLAN to access: Set the filter to disable all IP communications. <p>Certain packets may have been discarded by filtering, or packets may have been discarded through bandwidth monitoring, discarding control, or shaper of the QoS control. Check to see if the conditions of filtering and QoS control in the configuration have been set up correctly and if bandwidth monitoring, discarding control, or shaper has been set up appropriately for system operation. For the procedure, see "3.23.1 Checking Filtering/QoS Setting Information."</p>

3.13 Communication Failure on High-reliability Function

3.13.1 GSRP Communication Failures

If the communication is not possible in the GSRP configuration, isolate the problem according to the failure analysis method shown in the table below.

Table 3-58: Analysis Method for Communication Failure in GSRP Configuration

No.	Troubleshooting Steps and Command	Action
1	On this system and remote system constituting a GSRP group, check the status of the VLAN group to which the failed VLAN belongs using the <code>show gsrp</code> command.	Go to No. 2 if one system is master and the other system is non-master.
		If either system is Backup (No Neighbor), recover from the communication failure between direct links. GSRP Advertise frames may have been discarded by filtering, or GSRP Advertise frames may have been discarded through bandwidth monitoring, discarding control, or shaper of the QoS control. See "3.23.1 Checking Filtering/QoS Setting Information" to check for it. If necessary, change the system that is Backup (No Neighbor) to Master using the <code>set gsrp master</code> command.
		If both systems are Backup or Backup (Waiting), check to see if the master/backup selection method (Selection-Pattern) is the same between the systems.
		If both systems are Backup (Lock), reset the lock status of either or both systems.
		If both systems are Master, restart either GSRP program using the <code>restart gsrp</code> command.
	In other cases, temporary status transition is in progress. Wait for a while for the communication to recover.	
2	Check the status of the VLAN port on this system and systems on the communication path.	Restore the failed VLAN port on this system or systems on the communication path.
		If the conditions below are all met, activate the VLAN port using the <code>activate</code> command. <ul style="list-style-type: none"> The MAC address table flash method for the current VLAN port is "Reset" (determine by using the <code>show gsrp</code> command with "port" parameter specified).
		Go to No. 3 if there is no failure on the VLAN port of this system or systems on the communication path.
3	Check the MAC address table flash method (GSRP/Reset/No) to the VLAN port on this system using the <code>show gsrp</code> command with "port" parameter specified.	If the MAC address table flash method is either GSRP or Reset and does not match the configuration, correct it using configuration command <code>gsrp reset-flash-port</code> and <code>gsrp no-flash-port</code> .
		If the MAC address table flash method is either GSRP or Reset and matches the configuration, restart the GSRP program on this system with the <code>restart gsrp</code> command.
		If the MAC address table flash method is No, wait for aging of MAC address table on the neighboring system on the communication path.

If master/backup is not switched as expected in the GSRP configuration, isolate the problem using the failure analysis method shown in the table below.

3. Troubleshooting Functional Failures in Operation

Table 3-59: Analysis Method for Abnormal Status in GSRP Configuration

No.	Troubleshooting Steps and Command	Action
1	Check the status of the VLAN group in which master/backup is not switched as expected, using the <code>show gsrp</code> command.	Go to No. 2 if one system is master and the other system is non-master.
		If one of the systems is Backup (No Neighbor), recover from the communication failure between direct links. If necessary, change the system that is Backup (No Neighbor) to Master using the <code>set gsrp master</code> command.
		If both systems are Backup or Backup (Waiting), check to see if the master/backup selection method (Selection-Pattern) is the same between the systems.
		If both systems are Backup (Lock), reset the lock status of either one of the systems or both systems.
		If both systems are Master, restart one of GSRP programs using the <code>restart gsrp</code> command.
	In other cases, temporary status transition is in progress. Wait for a while.	
2	Check to see if the master/backup selection method (Selection-Pattern), the number of active ports (Active-Ports) on this system and the remote system, the priority information (Priority), and master/backup selection based on the MAC address are correct, using the <code>show gsrp</code> , <code>show gsrp</code> , and <code><GSRP-ID> vlan-group <VLAN group ID list></code> commands.	Go to No. 3 if the number of active ports (Active Ports) does not match the number of Up ports (Up Ports) although the items above are correct.
		Restart the GSRP program on this system using the <code>restart gsrp</code> command if the selection is incorrect.
3	Check the delay time until reflection to the active port is made (port-up-delay) and remaining delay time (delay) using the <code>show gsrp detail</code> and <code>show gsrp <GSRP-ID> port <Port list></code> commands.	If the delay time (port-ip-delay) is infinite (infinity), execute the <code>clear gsrp port-up-delay</code> command to reflect the number of Up ports (UP Ports) to the number of active ports (Active Ports).
		If delay time (port-up-delay) is not infinite (infinity) and the remaining delay time (delay) exists, wait until they are reflected after the remaining delay time is over. Execute the <code>clear gsrp port-up-delay</code> command for immediate reflection.

When detecting the reception timeout of GSRP Advertise in GSRP configuration causes unknown adjacency, isolate the cause according to the table below.

Table 3-60: Analysis Method for GSRP Unknown Adjacency

No.	Troubleshooting Steps and Command	Action
1	Check to see the transmission interval of GSRP Advertise frames (Advertise Interval) and the retaining period of GSRP Advertise frames (Advertise Hold Time) by using the <code>show gsrp detail</code> command.	When the retaining period of GSRP Advertise frames is the same or shorter than the transmission interval of GSRP advertise frames, set a bigger value in the retaining period of GSRP advertise frames than the transmission interval of GSRP Advertise frames.
		When the retaining period of GSRP Advertise frames is longer than the transmission interval of GSRP advertise frames, set a bigger value in the retaining period of GSRP advertise frames.
		Seeing " 3.23.1 Checking Filtering/QoS Setting Information ," check to see the factors that discard GSRP advertise frames (such as filters, bandwidth monitoring for QoS control, discard control, or shaper).

3.13.2 Communication with VRRP Configuration in IPv4 Network Is Disabled

Isolate the problem according to the failure analysis methods shown in the table below if communication with the VRRP configuration is disabled.

Table 3-61: VRRP Failure Analysis Method

No.	Troubleshooting Steps and Command	Action
1	Check the status of the remote systems and this system constituting a same virtual router and confirm that one system is used as a master router and other systems are used as backup routers.	<p>For the configuration constituting a single virtual router, if one system is master and the other systems are backup, check the following:</p> <ul style="list-style-type: none"> • If terminals are connected under the virtual router without other routers between them, confirm that the virtual IP address of the virtual router is configured as a default gateway in the network settings of each terminal. • Check for the routing information in devices on the communication paths including this system. <p>Go to No. 2 if there is no problem in terminal setting and in the route information in systems on the communication route.</p> <hr/> <p>Go to No. 3 if the status of a virtual router is not correct.</p>
2	Execute the <code>show vlan</code> command with "detail" parameter specified to confirm that the status of the physical port within the VLAN where the virtual router is set up is set to "Forwarding."	<ul style="list-style-type: none"> • If the physical port is set to "Blocking," the communication has been interrupted temporarily due to the STP topology change or the like. If this is the case, wait for a while and check again to see if the physical port is set to "Forwarding." If the status of the physical port does not change to "Forwarding" after some time, check the configuration and physical network structure. • If the physical port is "down," it is not physically connected. Check to see if connectors and/or cables are connected correctly. <hr/> <p>If the status of the physical port is "Forwarding," check to see if traffic in the target network is not high.</p>
3	Confirm that both remote system and this system constituting a virtual router are not set to master.	<p>Go to No. 4 if multiple virtual routers are set to master. [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]</p> <p>Go to No. 6 if multiple virtual routers are set to master. [IP8800/S3600]</p> <hr/> <p>Go to No. 10 if multiple virtual routers are not set to master.</p>
4	Confirm that primary virtual router to which virtual router connect is set by the detail parameter of the <code>show vrrpstatus</code> command. [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]	<p>If the primary virtual router is configured, go to No.5.</p> <hr/> <p>If the primary virtual router is not configured, go to No.6.</p>
5	Confirm that VLAN and VRID of the primary virtual router are the same as ones of devices connected to the virtual routers. [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]	<p>If VLAN and VRID of the primary virtual router are different among devices connected to the virtual routers, multiple of the virtual routers will function as master. Be sure to adjust the configurations of devices connected to virtual routers.</p> <hr/> <p>If VLAN and VRID of the primary virtual router are the same among devices connected to the virtual routers, go to No.6. Note that you should take those procedure (No.6 or later) against the primary router.</p>
6	Check the communication between the routers constituting the virtual router using the <code>ping</code> command with the actual IPv4 addresses.	<p>If the routers constituting the virtual router cannot communicate with each other with the actual IPv4 addresses, check the physical network configuration.</p> <hr/> <p>Go to No. 7, if the communication between routers constituting the virtual router is possible by issuing the <code>ping</code> command with the actual IPv4 addresses.</p>

3. Troubleshooting Functional Failures in Operation

No.	Troubleshooting Steps and Command	Action
7	Execute the <code>show logging</code> command and the <code>show vrrpstatus</code> command with "statistics" parameter specified to check the receiving status of the ADVERTISEMENT packets.	<ul style="list-style-type: none"> • If "Virtual router <VRID> of <Interface Name> received VRRP packet for which the advertisement interval is different than the one configured for local virtual router." is registered in the type log and "<Number of packets> with bad advertisement interval" of statistics is incremented, confirm that set values of the ADVERTISEMENT packet sending interval match between this system and the remote system. • If "Virtual router <VRID> of <Interface Name> received VRRP packet for which the advertisement interval is different than the one configured for local virtual router." is registered in the type log and "<Number of packets> with bad advertisement interval" of statistics is incremented, confirm that set values of the ADVERTISEMENT packet sending interval match between this system and the remote system. • If "Virtual router <VRID> of <Interface Name> received VRRP packet with IP TTL not equal to 255." is registered in the type log and "<Number of packets> with bad ip ttl" of statistics is incremented, confirm that there is no other router between this system and the remote system. • If "Virtual router <VRID> of <Interface Name> received VRRP packet for which the address list does not match the locally configured list for the virtual router." is registered in the type log and "<Number of packets> with bad ip address list" of statistics is incremented, confirm that settings of the virtual IP address are same. • If "Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check." is registered in the type log and "<Number of packets> with bad authentication type" of statistics is incremented, check to see that the authentication password has been set on this system and the remote system. • If "VRRP packet received with unsupported version number." is shown in the type log and statistics information "<Number of packets> with invalid type" is incremented, confirm that the VRRP mode between this system and remote system is same. <p>If the ADVERTISEMENT packet is normally received, check the remote system. Go to No. 8 if the ADVERTISEMENT packet is not received.</p>
8	Check the statistical information of the physical port to which the remote system constituting the same virtual router is connected using the <code>show interfaces</code> command. Also, check the CPU usage using the <code>show cpu</code> command.	<p>If "Input rate" and "Output rate" are excessive on the physical port to which the remote system is connected and the line traffic is high or the CPU usage checked by the <code>show cpu</code> command is high, take the following actions:</p> <ul style="list-style-type: none"> • If the line loops, review the use of STP or physical network configuration to eliminate the loop. • Execute configuration command <code>vrrp timers advertise</code> to set up rather long sending intervals for sending the ADVERTISEMENT packets. • Execute configuration command <code>vrrp preempt delay</code> to set the automatic switchback suppressing time. <p>Go to No. 9 if the traffic of the physical port is low.</p>
9	Confirm that discarding ADVERTISEMENT packets is not set in the filter setting.	<p>If such filtering setting exists, change the filtering setting so that the ADVERTISEMENT packets are not discarded.</p> <p>If this is not the case, check for the operation of the remote system constituting the same virtual router.</p>
10	If a failure monitoring interface has been set up, check for its status.	<p>If another virtual router is defined on the interface on which a failure monitoring interface is set up, confirm that the failure monitoring interface of that virtual router is not the interface of this virtual router. Otherwise, delete the setting on one of the failure interface.</p> <p>Go to No. 11 if the failure monitoring interface described above is not set up.</p>

No.	Troubleshooting Steps and Command	Action
11	Execute <code>show vrrpstatus</code> command with "detail" parameter specified to confirm that the virtual router status is not "Initial."	<p>If the virtual router is set to "Initial," check the following items:</p> <ul style="list-style-type: none"> • If the current priority is not set to zero (0), delete the non-operation factors displayed in the "Admin State" column. (For non-operation factors, see "Operation Commands.") • Execute the <code>show logging</code> command to check the log, and if "The VRRP virtual MAC address entry can't be registered at hardware tables" is displayed, setting up the hardware MAC address table is failed. Delete the configuration for the current virtual router and reconfigure the configuration with a different virtual router number, or modify the ID of the VLAN where the virtual router is set up, then the virtual router may operate. [IP8800/S3600] <p>If the virtual router is not set to "Initial," check the operation of the remote system constituting the same virtual router.</p>

3.13.3 Communication with VRRP Configuration in IPv6 Network Is Disabled

Isolate the problem according to the failure analysis methods shown in the table below if communication with the VRRP configuration is disabled.

Table 3-62: VRRP Failure Analysis Method

No.	Troubleshooting Steps and Command	Action
1	Check the status of the remote systems and this system constituting a same virtual router and confirm that one system is used as a master router and other systems are used as backup routers.	<p>For the configuration constituting a single virtual router, if one system is master and the other systems are backup, check the following:</p> <ul style="list-style-type: none"> • If terminals are connected under the virtual router without other routers between them, confirm that the virtual IP address of the virtual router is configured as a default gateway in the network settings of each terminal. • Check for the routing information in devices on the communication paths including this system. <p>Go to No. 2 if there is no problem in terminal setting and in the route information in systems on the communication route.</p> <p>Go to No. 3 if the status of a virtual router is not correct.</p>
2	Execute the <code>show vlan</code> command with "detail" parameter specified to confirm that the status of the physical port within the VLAN where the virtual router is set up is set to "Forwarding."	<ul style="list-style-type: none"> • If the physical port is set to "Blocking," the communication has been interrupted temporarily due to the STP topology change or the like. If this is the case, wait for a while and check again to see if the physical port is set to "Forwarding." If the status of the physical port does not change to "Forwarding" after some time, check the configuration and physical network structure. • If the physical port is "down," it is not physically connected. Check to see if connectors and/or cables are connected correctly. <p>If the status of the physical port is "Forwarding," check for the target network for the high traffic.</p>
3	Confirm that both remote system and this system constituting a virtual router are not set to master.	<p>Go to No. 4 if multiple virtual routers are set to master.</p> <p>Go to No. 8 if only one virtual router is set to master.</p>
4	Check the communication between the routers constituting the virtual router using the <code>ping ipv6</code> command with the actual IPv6 addresses.	<p>If the routers constituting the virtual router cannot communicate with each other with the actual IPv6 addresses, check the physical network configuration.</p> <p>Go to No. 5, if the communication between routers constituting the virtual router is possible by issuing the <code>ping ipv6</code> command with the actual IPv6 addresses.</p>

3. Troubleshooting Functional Failures in Operation

No.	Troubleshooting Steps and Command	Action
5	<p>Execute the <code>show vrrpstatus</code> command with "statistics" parameter specified to check the receiving status of ADVERTISEMENT packets.</p>	<ul style="list-style-type: none"> • If "Virtual router <VRID> of <Interface Name> received VRRP packet for which the advertisement interval is different than the one configured for local virtual router." is registered in the type log and "<Number of packets> with bad advertisement interval" of statistics is incremented, confirm that set values of the ADVERTISEMENT packet sending interval and the settings of the VRRP operation mode between this system and the remote system are same. • If "Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check." is registered in the type log and "<Number of packets> with authentication failed" of statistics is incremented, confirm that password settings match between this system and the remote system. • If "Virtual router <VRID> of <Interface Name> received VRRP packet with IP HopLimit not equal to 255." is registered in the type log and "<Number of packets> with bad ipv6 hoplimit" of statistics is incremented, confirm that there is no other router between this system and the remote system. • If "Virtual router <VRID> of <Interface Name> received VRRP packet for which the address list does not match the locally configured list for the virtual router." is registered in the type log and "<Number of packets> with bad ipv6 address list" of statistics is incremented, confirm that the settings of the virtual IP address and VRRP operation mode are same. • If "Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check." is registered in the type log and "<Number of packets> with bad authentication type" of statistics is incremented, check to see if the authentication password has been set on this system and the remote system. • If "Virtual router <VRID> of <Interface Name> received VRRP packet that length less than the length of the VRRP header." is registered in the type log and "<Number of packets> with packet length error" of statistics is incremented, confirm that settings of the VRRP operation mode between this system and the remote system are same. • When "VRRP packet received with unsupported version number." is registered in the type log and "<Number of packets> with invalid type" of statics is incremented, confirm that settings of the VRRP operation mode between this system and the remote system are same. <p>If the ADVERTISEMENT packet is normally received, check the remote system. Go to No. 6 if the ADVERTISEMENT packet is not received.</p>
6	<p>Check the statistical information of the physical port to which the remote system constituting the same virtual router is connected using the <code>show interfaces</code> command. Also, check the CPU usage using the <code>show cpu</code> command.</p>	<p>If "Input rate" and "Output rate" are excessive on the physical port to which the remote system is connected and the line traffic is high or the CPU usage checked by the <code>show cpu</code> command is high, take the following actions:</p> <ul style="list-style-type: none"> • If the line loops, review the use of STP or physical network configuration to eliminate the loop. • Execute configuration command <code>vrrp timers advertise</code> to set up rather long sending intervals for sending the ADVERTISEMENT packets. • Execute configuration command <code>vrrp preempt delay</code> to set the automatic switch back suppressing time. <p>Go to No. 7 if the traffic of the physical port is low.</p>
7	<p>Confirm that discarding ADVERTISEMENT packets is not set in the filter setting.</p>	<p>If such filtering setting exists, change the filtering setting so that the ADVERTISEMENT packets are not discarded.</p> <p>If this is not the case, check for the operation of the remote system constituting the same virtual router.</p>
8	<p>If a failure monitoring interface has been set up, check for its status.</p>	<p>If another virtual router is defined on the interface on which a failure monitoring interface is set up, confirm that the failure monitoring interface of that virtual router is not the interface of this virtual router. Otherwise, delete the setting of either failure interface.</p> <p>Go to No. 9 if the failure monitoring interface described above is not set up.</p>

No.	Troubleshooting Steps and Command	Action
9	Execute <code>show vrrpstatus</code> command with "detail" parameter specified to check the virtual router status.	<p>If the virtual router is set to "Initial," check the following items:</p> <ul style="list-style-type: none"> • If the current priority is not set to zero (0), delete the non-operation factors displayed in the "Admin State" column. (For non-operation factors, see "Operation Commands.") • Execute the <code>show logging</code> command to check the log, and if "The VRRP virtual MAC address entry can't be registered at hardware tables" is displayed, setting up the hardware MAC address table failed. Delete the configuration for the current virtual router and reconfigure the configuration with a different virtual router number, or modify the ID of the VLAN where the virtual router is set up, and the virtual router may operate. [IP8800/S3600] <hr/> <p>If the virtual router is not set to "Initial," check the operation of the remote system constituting the same virtual router.</p>

3.14 SNMP Communication Failure

3.14.1 MIBs Cannot Be Obtained from SNMP Manager

Confirm that the configuration has been set correctly.

When using SNMPv1 or SNMPv2C

Execute the `show access-list` command to confirm that the IP address of the SNMP manager has been registered on the access list in the configuration. Execute the `show snmp-server` command to confirm that the community name and access list have been registered correctly.

If they are not registered, execute configuration command `snmp-server community` to set up the information on the SNMP manager.

```
(config)# show access-list
access-list enable
access-list 1 permit ip 20.1.1.1 0.0.0.255
!
(config)# show snmp-server
snmp-server community "event-monitor" ro 1
!
(config)#
```

When using SNMPv3

Execute the `show snmp-server` command to confirm that the information on the SNMP manager has been registered in the configuration for this system. If it is not correctly registered, execute the configuration command below to set up the information on the SNMP manager.

- `snmp-server engineID local`
- `snmp-server view`
- `snmp-server user`
- `snmp-server group`

```
(config)# show snmp-server
snmp-server engineID local "engine-ID"
snmp-server group "v3group" v3 priv read "view1" write "view1"
snmp-server user "v3user" "v3group" v3 auth md5 "abc*_1234" priv des "xyz/
+6789"
snmp-server view "view1" 1.3.6.1.2.1.1 included
!
(config)#
```

3.14.2 Traps Cannot Be Received by SNMP Manager

Confirm that the configuration has been set correctly.

When using SNMPv1 or SNMPv2C

Execute configuration command `show snmp-server` to confirm that the information on the SNMP manager and trap has been registered in the configuration for this system.

If it is not registered, execute configuration command `snmp-server host` to set up the information on the SNMP manager and trap.

```
(config)# show snmp-server
snmp-server host 20.1.1.1 traps "event-monitor" snmp
!
(config)#
```

When using SNMPv3

Execute the `show snmp-server` command to confirm that the information on the SNMP manager and trap has been registered in the configuration for this system. If it is not correctly registered, execute the configuration command below to set up the information on the SNMP manager and trap.

- `snmp-server engineID local`
- `snmp-server view`
- `snmp-server user`
- `snmp-server group`
- `snmp-server host`

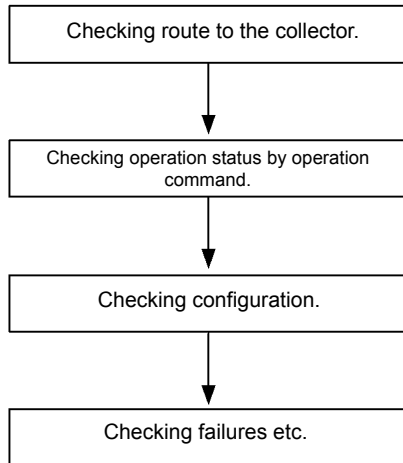
```
(config)# show snmp-server
snmp-server engineID local "engine-ID"
snmp-server group "v3group" v3 priv notify "view1"
snmp-server host 20.1.1.1 traps "v3user" version 3 priv snmp
snmp-server user "v3user" "v3group" v3 auth md5 "abc*_1234" priv des "xyz/
+6789"
snmp-server view "view1" 1.3.6.1 included
!
(config)#
```

In some SNMP manager systems, "ospf" or "bgp" traps issued by SNMPv2C or SNMPv3 may not be received. For such systems, review the trap receiving settings on the SNMP manager in accordance with object ID for each trap described in "MIB Reference."

3.15 Troubleshooting of sFlow Statistics (Flow Statistics) Function

The flow for troubleshooting of sFlow statistics function in this system is as follows.

Figure 3-18: Troubleshooting Flow of sFlow Statistics Function



3.15.1 sFlow Packets Do Not Reach Collector

(1) Checking route to the collector

See "[3.6.1 Communication Is Disabled or Is Disconnected](#)" and "[3.9.1 Communication Is Disabled or Is Disconnected](#)" to check to see if the collector is properly connected to network. If the maximum size of sFlow packets (max-packet-size) is changed with the configuration, check to see if the connection to the collector can be established with the specified packet size.

(2) Checking operation status by operation command

Execute the `show sflow` command several times to display the sFlow statistical information and check to see if sFlow statistics function operates normally. If the underlined values shown below are not incremented, see "[\(3\)Checking configuration.](#)" If incremented, see "[3.6.1 Communication Is Disabled or Is Disconnected,](#)" "[3.9.1 Communication Is Disabled or Is Disconnected](#)" and "[\(5\)Checking settings of collector](#)" to check to see if the collector is properly connected to network.

Figure 3-19: Display Example of show sflow Command

```

> show sflow
Date 2006/10/24 20:04:01 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 16:00:05
sFlow agent data :
  sFlow service version : 4
  CounterSample interval rate: 60 seconds
  Default configured rate: 1 per 2048 packets
  Default actual rate : 1 per 2048 packets
  Configured sFlow ingress ports : 1/ 2-4
  Configured sFlow egress ports : 5/ 9-11
  Received sFlow samples : 37269 Dropped sFlow samples(Dropped Que) :
  
```

```

2093(2041)
  Exported sFlow samples : 37269   Couldn't exported sFlow samples   :      0
sFlow collector data :
  Collector IP address: 192.168.4.199  UDP:6343  Source IP address: 130.130.130.1
  Send FlowSample UDP packets   : 12077  Send failed packets:      0
  Send CounterSample UDP packets: 621   Send failed packets:      0
  Collector IP address: 192.168.4.203  UDP:65535 Source IP address: 130.130.130.1
  Send FlowSample UDP packets   : 12077  Send failed packets:      0
  Send CounterSample UDP packets: 621   Send failed packets:      0
>

```

Note: Confirm that the underlined values are incremented.

(3) Checking configuration

Check the configuration in operation on the following points:

- Check that the IP address and UDP port number of the sFlow packet destination collector are set correctly in configuration.

Figure 3-20: Display Example Configuration 1

```

(config)# show sflow
sflow destination 192.1.1.1 6455   <- Collector information must be set correctly.
sflow sample 2048
!
(config)#

```

- Check that the sampling interval is set.
If the sampling interval is not set, the system operates with default value (large value), which is so large that flow sample is seldom sent to the collector. Set the appropriate sampling interval. However, if the value extremely smaller than the recommended value is set, the CPU usage may be raised.

Figure 3-21: Display Example of Configuration 2

```

(config)# show sflow
sflow destination 192.1.1.1 6455
sflow sample 2048   <- Appropriate sampling interval must be set.
!
(config)#

```

Figure 3-22: Display Example of Operation Command

```

> show sflow
Date 2006/10/24 20:04:01 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 16:00:05
  sFlow agent data :
    sFlow service version : 4
    CounterSample interval rate: 60 seconds
    Default configured rate: 1 per 2048 packets
    Default actual rate   : 1 per 2048 packets
    Configured sFlow ingress ports : 1/ 2-4
    Configured sFlow egress ports  : 5/ 9-11
    Received sFlow samples : 37269  Dropped sFlow samples(Dropped Que) :
2093(2041)
  Exported sFlow samples : 37269  Couldn't exported sFlow samples   :      0
  :
>

```

Note: Confirm that the appropriate sampling interval is displayed at the underlined part.

- Confirm that `sflow forward` is set for the physical port subject to flow statistics.

Figure 3-23: Display Example of Configuration 3

```
(config)# show interfaces
interface gigabitethernet 1/2
  switchport mode access
  sflow forward ingress      <- sflow forward must be set here.
!
(config)#
```

- See ["3.23.1 Checking Filtering/QoS Setting Information"](#) to confirm that "filter" is not set for the physical port subject to flow statistics.
- Specifying Source IP address for sFlow packets with "sflow source," check to see if the IP address is assigned to the port of this system.

Figure 3-24: Display Example of Configuration 4

```
(config)# show sflow
sflow destination 192.1.1.1 6455
sflow sample 2048
sflow source 192.1.1.100 <- This IP address must be one assigned to the port of
this system.
!
(config)#
```

(4) Checking NIF/port status

Execute the `show interfaces` command to check that up/down status of the physical port of this system or the physical port connecting to the collector to be monitored by sFlow statistics is "active" (normal operation).

Figure 3-25: Display Example of Port Status

```
> show interfaces gigabitethernet 1/5
Date 2006/10/24 17:19:34 UTC
NIF1: active 48-port 10BASE-T/100BASE-TX/1000BASE-T  retry:0
  Average:150Mbps/24Gbps  Peak:200Mbps at 15:44:37
Port5: active up 100BASE-TX full(auto) 0012.e220.ec31
  Time-since-last-status-change:1:47:47
  Bandwidth:10000kbps  Average out:5Mbps  Average in:5Mbps
  Peak out:5Mbps at 15:44:36  Peak in:5Mbps at 15:44:18
  Output rate: 4893.5kbps 16.8kpps
  Input rate: 4893.5kbps 16.8kpps
  Flow control send :off
  Flow control receive:off
  TPID:8100
:
```

Note: Confirm that "active" or "active up" is displayed at the underlined part.

If the port status is DOWN, see ["3.6.1 Communication Is Disabled or Is Disconnected"](#) and ["3.9.1 Communication Is Disabled or Is Disconnected."](#)

(5) Checking settings of collector

- Confirm that the UDP port number (default: 6343) on the collector side is available to receive packets. If the port is not ready for receiving packets, ICMP ([Type]Destination Unreachable [Code]Port Unreachable) will be transmitted to this system.
- Confirm that other settings on the collector used are correct.

3.15.2 Flow Sample Does Not Reach Collector

If problem still persists even after checking "3.15.1 sFlow Packets Do Not Reach Collector," check the following:

(1) Checking presence/absence of the relay packet

Execute the `show interfaces` command to check to see if the packet is relayed.

Figure 3-26: Display Example of Port Status

```
> show interfaces gigabitethernet 1/5
Date 2006/10/24 17:19:34 UTC
NIF1: active 48-port 10BASE-T/100BASE-TX/1000BASE-T retry:0
      Average:150Mbps/24Gbps Peak:200Mbps at 15:44:37
Port5: active up 100BASE-TX full(auto) 0012.e220.ec31
      Time-since-last-status-change:1:47:47
      Bandwidth:10000kbps Average out:5Mbps Average in:5Mbps
      Peak out:5Mbps at 15:44:36 Peak in:5Mbps at 15:44:18
      Output rate: 4893.5kbps 16.8kpps
      Input rate: 4893.5kbps 16.8kpps
      Flow control send :off
      Flow control receive:off
      TPID:8100
:
```

>

Note: Confirm that the packet is relayed based on the display at underlined part.

(2) Checking settings of collector

Check to see if settings of the collector used are correct.

3.15.3 Counter Sample Does Not Reach Collector

If problem still persists even after checking "3.15.1 sFlow Packets Do Not Reach Collector," check the following:

(1) Checking transmission interval of counter sample

Check to see if the transmission interval of the counter sample related to flow statistics is set to 0 in the configuration of this system. If set to 0, the counter sample data is not sent to the collector.

Figure 3-27: Display Example of Configuration

```
(config)# show sflow
sflow destination 192.1.1.1 6455
sflow sample 2048
sflow polling-interval 60 <- 0 must not be set here.
!
(config)#
```

3.16 Communication Failures on Neighboring System Managing Function

3.16.1 Unable to Obtain Neighboring System Information via LLDP Function

If it is not possible to acquire correctly neighbor system information with LLDP functions, isolate the problem using the failure analysis method shown in the table below.

Table 3-63: Failure Analysis Method When Using LLDP Functions

No.	Troubleshooting Steps and Command	Action
1	Check the status of LLDP functions using the <code>show lldp</code> command.	If "Status" is "Enabled," go to No. 2.
		If "Status" is "Disabled," the LLDP function is disabled. Enable the LLDP function.
2	Execute the <code>show lldp</code> command to check the port information.	If the information on the port to which the neighboring system is connected appears, go to No. 3.
		If the information on the port to which the neighboring system is connected does not appear, the port is not covered by the LLDP function. Enable the LLDP function for the port.
3	Execute the <code>show lldp statistics</code> command to check for the statistics on the port to which the neighboring system is connected.	If the Tx count has been incremented while the Rx has not, also check No. 1 through 3 on the neighboring system. If the Tx count also has been incremented on the neighboring system, check the connection, since the systems may be incorrectly connected.
		If the Discard count has been incremented, check the connection between the systems.
		Otherwise, go to No. 4.
4	Execute the <code>show lldp</code> command to check the status of the port to which the neighboring system is connected.	If the Link has been established, go to No. 5.
		If the Link is Down, check the line status. For checking the status, see "3.4 Network Interface Communication Failure."
5	Execute the <code>show lldp</code> command to check the number of neighboring system information on the port to which the neighboring system is connected.	If "Neighbor Counts" is zero (0), check No. 1 through 5 on the neighboring system. If the number of the neighboring system information is also set to zero (0) on the neighboring system, check the connection since it may be incorrect. LLDP control frames may have been discarded by filtering or QoS control. See "3.23.1 Checking Filtering/QoS Setting Information" to check for it.

3.16.2 Unable to Obtain Neighboring System Information via OADP Function

If it is not possible to acquire the neighboring system information correctly with the OADP function, isolate the problem using the failure analysis method shown in the table below.

Table 3-64: Failure Analysis When Using OADP Function

No.	Troubleshooting Steps and Command	Action
1	Execute the <code>show oadp</code> command to check the OADP operation.	If "Status" is "Enabled," go to No. 2.
		If "Status" is "Disabled," the OADP function is disabled. Enable the OADP function.

No.	Troubleshooting Steps and Command	Action
2	Execute the <code>show oadp</code> command to check the port information displayed.	<p>If the information on the port to which the neighboring system is connected appears in "Enabled Port," go to No. 3.</p> <p>If the information on the port to which the neighboring system is connected does not appear in "Enabled Port," the port is not covered by the OADP function. Enable the OADP function for the port. Note that the OADP function is disabled for the ports included in a channel group. Enable the OADP function for the channel group.</p>
3	Execute the <code>show oadp statistics</code> command to check for the statistics on the port to which the neighboring system is connected.	<p>If the Tx count has been incremented while the Rx has not, also check No. 1 through 3 on the neighboring system. If the Tx count also has been incremented on the neighboring system, check the connection, since the systems may be incorrectly connected.</p> <p>If the Discard/ERR count has been incremented, check the connection between the systems.</p> <p>Otherwise, go to No. 4.</p>
4	Execute the <code>show interfaces</code> command to check the status of the port to which the neighboring system is connected.	<p>If the port status is "active up," go to No. 5.</p> <p>Otherwise, see "3.4 Network Interface Communication Failure."</p>
5	Execute the <code>show vlan</code> command to check the status of the VLAN containing the port to which the neighboring system is connected.	<p>If "Status" is "Up," go to No. 6.</p> <p>If "Status" is "Disabled," it is not covered by the OADP function. Enable the VLAN state.</p> <p>Otherwise, see "3.5 Layer 2 Network Communication Failure."</p>
6	Execute the <code>show oadp</code> command to check neighboring system information on the port to which neighboring system is connected.	<p>If no information is displayed, check No. 1 through 6 on the neighboring system. If the neighboring system information is not displayed on the neighboring system, connection between systems may be incorrect. Therefore, check the connection. OADP control frames may have been discarded by filtering or QoS control. See "3.23.1 Checking Filtering/QoS Setting Information" to check for it.</p>

3.17 NTP Communication Failure

3.17.1 Time Synchronization by NTP Is Disabled

If time synchronization by NTP is disabled, isolate the problem by following the failure analysis methods shown in the table below.

Table 3-65: NTP Failure Analysis Method

No.	Troubleshooting Steps and Command	Action
1	Execute the <code>show clock</code> command to see if a time zone has been set up.	If the command retrieves the time zone setting, go to No. 2.
		If no time zone has been set up in the output of the command, set up a time zone.
2	Check the difference in time between this system and the NTP server.	Go to No. 3 if the difference in time between this system and the NTP server is within 1000 seconds.
		If the difference in time between this system and the NTP server is greater than 1000 seconds, adjust the time of this system with the time of the NTP server using the <code>set clock</code> command.
3	Check communication with the NTP server by IPv4.	Execute the <code>ping</code> command to see if NTP server and this system can communicate over IPv4 protocol.
		Confirm that no setting for discarding packets using UDP port number 123 exists in the NTP server or this system.

3.18 Communication Failure on IEEE802.3ah/UDLD Function

3.18.1 Port Becomes Inactive Due to IEEE802.3ah/UDLD Function

If the port becomes inactive due to IEEE802.3ah/UDLD function, isolate the problem by following failure analysis methods shown in the table below.

Table 3-66: Failure Analysis Method When IEEE802.3ah/UDLD Function Is in Use

No.	Troubleshooting Steps and Command	Action
1	Use the <code>show efmOAM</code> command to check the failure type of the port which becomes inactive due to IEEE802.3ah/UDLD function.	If "Down(loop)" is displayed in Link status, the network configuration which causes L2 loop may be adopted. Review the network configuration.
		If "Down(uni-link)" is displayed in Link status, go to No. 2.
2	Check that IEEE802.3ah/OAM function is enabled in the opposite system.	If not enabled, enable IEEE802.3ah/OAM function in the opposite system.
		If enabled, go to No. 3.
3	Execute the <code>show efmOAM statistics</code> command to check the inhibited configuration is not adopted.	If Unstable of Info TLV has been incremented, the configuration inhibited for IEEE802.3ah/UDLD function may be adopted. Check that the physical port is connected to only one system.
		If Unstable of Info TLV has not been incremented, go to No. 4.
4	Check that the system is directly connected to the opposite system.	If the system is connected through the media converter or hub, review the network configuration so that it is directly connected to the opposite system. If it cannot be avoided to use some relay equipment, use the media converter which enables the linkage status to be same at both sides (however, not recommended).
		If the system is directly connected to the opposite system, go to No. 5.
5	Execute the <code>show efmOAM</code> command to check the number of response timeout times for detecting the failure.	If the value of "udld-detection-count" is less than the initial value, the possibility that the one-way link failure is detected erroneously in spite of no actual failure is raised. Change the value of "udld-detection-count."
		If the value of "udld-detection-count" exceeds the initial value, go to No. 6.
6	Check settings of the filter and QoS control.	Control frames (slow-protocol) used by IEEE802.3ah/UDLD function may have been discarded by filtering or QoS control. See "3.23.1 Checking Filtering/QoS Setting Information" to check for it. If there is no problem, go to No. 7.
7	Test the line.	Test the line by referencing "6.1 Testing Line." If there is no problem, go to No. 8.
8	Check the cable.	Cable may be defective. Replace the cable used at the port.

Note:

IEEE802.3ah/OAM: OAM protocol specified by IEEE802.3ah.

IEEE802.3ah/UDLD: One-way link failure detection function specific to this system using IEEE802.3ah/OAM.

3.19 Problems on Redundant Configuration of Basic Control Unit (BCU)/Control and Switching Unit (CSU)/Management and Switching Unit (MSU) [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]

3.19.1 Active System Switchover Is Disabled

If switch between the active system and standby system is disabled, follow instructions in the table below.

Table 3-67: Problems and Actions When Switching Active System

No.	Cause for Switchover Disabled	Troubleshooting Steps	
1	The standby system is not activated. Check the STATUS LED on the standby system.	Lit in red	The standby system has failed. Replace the standby system BCU, CSU, or MSU board.
		OFF or lit in orange	Board is not activated. Execute the <code>inactivate standby/activate standby</code> command on the active system to activate the standby system.
		Blinking in green	The standby system is being activated. Wait a while until lit in green.
		Lit in green	The standby system is already activated, and another cause may exist. See other items.
2	The standby system is not prepared for switch. Login the active system, and use the <code>show system</code> command to check the status of the standby system.	fault	Any one of the followings is applied: <ul style="list-style-type: none"> • Activation of the standby system failed. • Inhibited combination of the active system board and standby system board is adopted. Eliminate the cause for failure, and restart the system. • Unavailable configuration has been set. Review settings in the configuration. Otherwise, see No. 1.
		inactive	Activation of the standby system is suppressed. Execute the <code>activate standby</code> command to activate the standby system.
		notconnect	The standby system is not installed. Install the standby system, then execute the <code>activate standby</code> command to activate the standby system.
		initialize	Activation of the standby system is not completed. Wait until activation completes.
		active or standby	Another cause may exist. See other items.
3	Modifying configuration. If the operation command is used to switchover, command execution fails.	During modifying configuration, switchover by the operation command is suppressed. Execute configuration command <code>status</code> on the active system to make all users working with configuration log out, then switch over the system by the operation command.	

3.20 Problems on Redundant Configuration of Basic Switching Unit (BSU) [IP8800/S6700]

3.20.1 Active BSU Switchover Is Disabled

If BSU cannot be switched in the redundant configuration, follow the instruction shown below.

1. Checking log
For the log, see the manual "Message Log Reference."
2. Isolating the problem according to the BSU operation status
Check the BSU operation status by using the `show system` command, and isolate the problem according to the table below.

Table 3-68: Failure Analysis Method When BSU Switchover Disabled

No.	BSU Operation Status	Problem	Action
1	active (not standby hot, standby cold, standby cold2)	The number of BSU boards set in configuration command <code>redundancy max-bsu</code> does not match the number of BSU boards which are to be operated as the active BSU.	Use configuration command <code>redundancy max-bsu</code> to set the number of BSU boards to be operated as the active BSU.
		BSU boards to be standby BSU are not installed.	Install the BSU boards.
2	fault	Unavailable configuration has been set.	Use configuration command <code>fldm prefer</code> to set flow distribution pattern of the filter and QoS function correctly. Use configuration command <code>fwdm prefer</code> to correctly set the distribution pattern of the maximum number of entries per device.
		The BSU is faulty.	According to the log of the BSU displayed by the <code>show logging</code> command, see the corresponding part in manual "Message Log Reference" and follow [Action] described.
3	inactive	The <code>inactivate bsu</code> command is set.	Use the <code>activate bsu</code> command to make the BSU active, standby hot, standby cold status, or standby cold status2.
		The setting by Configuration command <code>redundancy bsu-load-balancing smac</code> or <code>redundancy bsu-mode fixed</code> exists.	Delete the setting by Configuration command <code>redundancy bsu-load-balancing smac</code> or <code>redundancy bsu-mode fixed</code> and restart the system. For more details, see the manual "Configuration Settings."
		The BSU is not fully inserted.	Install the BSU board correctly.
		Different types of BSUs are installed together.	Unify the type of all BSU boards.
		BSU not supported by the software version is installed.	Check the BSU board type and software version. Replace the BSU board or update the software.
		BSU not supported by this device is installed.	Replace the BSU board.

3. Troubleshooting Functional Failures in Operation

No.	BSU Operation Status	Problem	Action
4	notconnect	The BSU is not installed.	Check if as many BSU boards as required for active BSU + standby BSU (if standby BSU is not required, only active BSU) are installed. If installed, no action is required. If not so, install the required number of BSU boards.
5	initialize	The BSU is being initialized.	Wait until initialization completes.
6	disable	no power enable is set by configuration command.	After checking that the BSU board to be used is installed, use configuration command <code>power enable</code> to make the BSU active, standby hot, standby cold status, or standby cold status2.

3.21 Problems on Power Saving Feature

3.21.1 Schedule Is Disabled [IP8800/S6700] [IP8800/S6600]

If schedule is disabled, follow the instruction shown below.

1. Check to see if the current time is included in the displayed schedule by using the `show power-control schedule` command, and isolate the problem according to the table below.

Table 3-69: Problems and Actions When Using Power Saving Feature with Power Saving Feature

No.	Display of Result	Confirmation	Cause	Action
1	Current time is not included	Check to see the setting by configuration command <code>schedule-power-control time-range</code>	The setting by configuration command <code>schedule-power-control time-range</code> is incorrect.	<ul style="list-style-type: none"> • Specify the time including the current time if not. • If an entry including the current time is set to disabled, delete the entry that is set to disabled.
2	Current time is included	Check to see if the feature specified by configuration command <code>schedule-power-control</code> and the feature specified during normal hours both are not matched. If it is same, see the Cause and Action.	The features assigned by configuration command <code>schedule-power-control</code> is already operating.	Check to see the setting of the configuration command <code>schedule-power-control</code> .
3		Using the <code>show system</code> command, check to see if "changing suspended" appears in the status of BSU/PSP. If so, see the Cause and Action.	The shortage of the number of operating BSUs/PSPs occurs.	To control the power of BSU/PSP, make redundant configuration of BSU/CSU. For information on redundant configuration, see the manual "Configuration Settings."
4		Using the <code>show logging</code> command, confirm that there is no change on the system time within 30 minutes before the start and end times of the schedule.	Schedule error caused by system time change occurs.	Wait for a while because the schedule will start within 30 minutes. For notices regarding time change, see the manual "Configuration Settings."

3.22 Congestion Caused by Packets Processed Through CPU Is Not Recovered

This section describes the procedure when congestion caused by packets requiring the handling of CPU is not recovered.

When a large amount of the packets requiring software process are received, the overflow on the receiving queue to CPU will cause the packet congestion.

The following message is displayed when the system detects packet congestion.

```
"E3 SOFTWARE 00003301 1000:000000000000 CPU congestion detected."
```

The following message is displayed when packet congestion is recovered.

```
"E3 SOFTWARE 00003302 1000:000000000000 CPU has recovered from congestion."
```

Congestion of packets handled by CPU might occur even in a normal condition because of unexpected reason such as CPU received a large amount of unknown packets caused by routing information aging for temporary. If the packet congestion is not recovered or the packet congestion occurs and is recovered repeatedly, the settings of this system or the network configuration might be wrong. Take the following procedures while the problem occurs.

Table 3-70: Problems and Actions When CPU Packets Congestion is not Recovered

No.	Troubleshooting Steps and Command	Action
1	Determine the type of packets <ul style="list-style-type: none"> Execute the <code>show netstat statistics</code> command at an interval of 20 seconds. Then, compare the results. 	Considering each of the results, if the count in "total packets received" as a statistics item of "ip" or "ip6" in the packet type is drastically incremented, go to No.2.
		Considering each of the results, if the count in "packets received" as a statistics item of "arp" in the packet type is drastically incremented, go to No.2.
		Otherwise, go to No.4.
2	Determine receiving VLAN interface <ul style="list-style-type: none"> Execute the <code>show netstat interface</code> command at an interval of 20 seconds. Then, compare the results. 	Considering each of the results, if the count in "Ipkts" as a statistics item in a specific VLAN interface is drastically incremented, go to No.3.
		Otherwise, go to No.4.
3	Specify source and destination addresses for packets <ul style="list-style-type: none"> Execute the <code>show tcpdump interface</code> command against VLAN interface specified in No.2. And then check to see source address and destination address in the packet type specified in No.1. 	If the destination address of packets whose packet type is "ip" or "ip6" is the same as this system's address, the packet might be transmitted illegally. Review the setting of the terminal having the source address or the network configurations to keep the terminal from sending the packets to this system.
		If the destination address of packets whose packet type is "ip" or "ip6" is the same as other system's address, it might be considered that addresses in arp information are not be resolved or a large amount of unknown destination packets are received. <ul style="list-style-type: none"> If packet type is "ip," see "(5)Checking ARP resolution information with neighboring system" in "3.6.1 Communication Is Disabled or Is Disconnected." If packet type is "ip6," see "(4)Checking NDP resolution information with neighboring system" in "3.9.1 Communication Is Disabled or Is Disconnected."
		If packet type is "arp," a large amount of arp packets are being received. In this case, L2 loop might occur. Review the network configurations. If no problem is found in the network configuration, review the setting of the terminal having the source address.

No.	Troubleshooting Steps and Command	Action
4	<p>Collecting analysis information</p> <ul style="list-style-type: none"> • Execute the <code>show tech-support</code> command and the <code>dump bsu</code> command in this order for two times. [IP8800/S6700] • Execute the <code>show tech-support</code> command and the <code>dump psp</code> command in this order for two times. [IP8800/S6600] [IP8800/S6300] • Execute the <code>show tech-support</code> command for two times. [IP8800/S3600] [IP8800/S2400] <p>Note</p> <ul style="list-style-type: none"> • When executing the <code>dump bsu</code> command or the <code>dump psp</code> command, do not execute the next command until the log appears indicating memory dump file collection has been completed. [IP8800/S6700] [IP8800/S6600] [IP8800/S6300] • Before executing the <code>dump bsu</code> command or the <code>dump psp</code> command for the second time, put aside the memory dump file created for the first time because executing the command clears the file created in the previous time. [IP8800/S6700] [IP8800/S6600] [IP8800/S6300] 	Send the collected information to the support division.

3.23 Communication Failure Caused by Settings of Filtering/QoS

3.23.1 Checking Filtering/QoS Setting Information

As a cause for communication failure on the network using this system, certain packets may have been discarded by filtering or packets may have been discarded through bandwidth monitoring, discarding control, or shaper of the QoS control.

If packets are discarded within this system by filtering or QoS control, the procedure for identifying the discarding location is described below.

(1) Checking packet discarding by filtering

1. Log in to the system.
2. Check the filtering conditions of the access list applied to the interface, the number of packets meeting the filtering conditions, and the number of packets discarded according to implicit discarding filter entry by using the `show access-filter` command.
3. Compare the filtering conditions identified in step 2 and the contents of the packet that cannot be exchanged, and see if the packets have been discarded. If the packets that cannot be exchanged do not meet all of the filtering conditions applied, the packets in this example, may have been implicitly discarded.
4. Review to see if setting conditions in filtering configuration are correct.

(2) Checking packet discarding through bandwidth monitoring of QoS control

1. Log in to the system.
2. Check the flow detecting condition and operation designation of bandwidth monitoring applied to the interface and the number of packets meeting the flow detecting conditions by executing the `show qos-flow` command.
3. Compare the flow detecting conditions identified in step 2 and the contents of the packet that cannot be exchanged, and see if the packets have been discarded. The packets which violate maximum bandwidth control are discarded, and "matched packets (max-rate over)" statistical information is incremented. If this statistical information is incremented, packets may be discarded through bandwidth monitoring applied to the interface.
4. Review to see if setting conditions in QoS control configuration are correct and bandwidth monitoring settings in system configuration are proper.

(3) Checking packet discarding through discarding control and shaper of QoS control

IP8800/S6700, IP8800/S6600, and IP8800/S6300

1. Log in to the system.
2. Check the "discard_pkt" statistical information of the port sending/receiving queue for the input interface and output interface used for communication by using the `show qos queueing` command with "interface" parameter specified.
3. Check the "discard_pkt" statistical information of the distribution sending/receiving queue for accommodating the input interface or output interface used for communication by using the `show qos queueing` command with "distribution" parameter specified.
4. If the statistical information identified in steps 2 and 3 is incremented, packets are discarded through discarding control of QoS control.
5. Review to see if discard control and shaper have been set up appropriately for the system operation.

IP8800/S3600 and IP8800/S2400

1. Log in to the system.
2. Check the "discard packets" statistical information of the output interface using the `show qos queueing` command.
3. If the statistical information identified in step 2 is incremented, packets are discarded through discarding control and shaper of QoS control.
4. Review to see if discard control and shaper have been set up appropriately for the system operation.

IP8800/S6700, IP8800/S6600, and IP8800/S6300

1. Log in to the system.
2. Specify port list in the `show shaper` command and check the "discard_pkt" statistical information on user queue of the input and output interfaces used for communication.
3. Specify interfaces in the `show qos queueing` command and check the "discard_pkt" statistical information on the port transmission/reception queue of the input and output interfaces used for communication.
4. Specify interfaces in the `show qos queueing` command and check the "discard_pkt" statistical information on the distribution transmission/reception queue of the input and output interfaces used for communication.
5. If the statistical information identified in step 2 to 4 is incremented, packets are discarded through discarding control of QoS control.
6. Review to see if discard control and shaper have been set up appropriately for the system operation.

4

Troubleshooting Communication Failures Due to Resource Shortage **[IP8800/S6700] [IP8800/S6600] [IP8800/S6300]**

[4.1 MAC Address Table Resource Shortage](#)

[4.2 When Resource Shortage of VLAN Identification Table Occurs](#)

[4.3 When Resource Shortage Occurs in Shared Memory](#)

4.1 MAC Address Table Resource Shortage

4.1.1 Checking Resource Usage of MAC Address Table

This system outputs operation log messages when the MAC address table usage reaches 80% and 100% of the accommodating condition. The operation log message output is shown in the table below.

Table 4-1: Operation Log Message for Checking Resource Usage

No.	Trigger	Log Message
1	When MAC address table usage reaches 80%	MAC address table entries was beyond 80 percent of capacity.
2	When MAC address table usage reaches 100%	MAC address table entries exceeded capacity.

Communication is not immediately affected when usage reaches 80%. However, if usage of MAC address table continuously increases, the limit accommodating condition may be reached and resource shortage resulting in disabled MAC address learning may arise. Check the set value and accommodation value in advance so that the limit of the accommodating condition will not be exceeded.

The MAC address table usage can be checked using the show system command (for details, see the manual "Operation Commands").

4.1.2 Action to Be Taken When MAC Address Table Resource Shortage Occurs

When usage of MAC address table reaches the limit of the accommodating condition, the corresponding log message is output at the timing listed in the table below.

Table 4-2: Operation Log Message for Checking Resource Use Status

No.	Trigger	Log Message
1	MAC address learning ARP/NDP learning	MAC address table entries exceeded capacity.
2	Static ARP/NDP registration	MAC address table entries exceeded capacity.
3	Static MAC address registration	The static MAC address entry can't be registered at MAC address table. (VLAN <ID>,mac <MAC>)*
4	Setting MAC address learning suppression function	The "no mac-address-table learning" entry can't be registered at MAC address table. (VLAN <ID>)*
5	IEEE802.1X authentication (port authentication, VLAN authentication (static))	The 802.1X Supplicant MAC address can't be registered at hardware tables.* Note: This log is displayed when the show dot1x logging command is executed.
6	Ring Protocol enabled Additional Ring Protocol registration	AXRP <ring id> : The MAC address entry can't be registered at hardware tables.
7	IGMP Snooping registration	IGMP snooping: The number of the IGMP snooping entry exceeded the capacity of this system.
8	MLD Snooping registration	MLD snooping: The number of the MLD snooping entry exceeded the capacity of this system.

No.	Trigger	Log Message
9	Web authentication (Static VLAN mode)	The login failed because of hardware restriction. Note: This log is displayed when the <code>show web-authentication logging</code> command is executed.
10	MAC authentication	The login failed because of hardware restriction. Note: This log is displayed when the <code>show mac-authentication logging</code> command is executed.

* The log message of No. 1 may be output at the same time.

If these log messages are output, the function that newly uses the MAC address table cannot be set. Review the network configuration and set the configuration allowing for operation below the limit of the system's accommodating condition.

No. 2, 3, 4 and 6 in the above table shows that setting cannot be registered to the MAC address table by the configuration command. No. 5 shows that setting cannot be registered to the MAC address table of the authenticated terminal (authentication failed). For re-configuration, follow the steps below.

1. Review that configuration so that new entries will not be registered by MAC address learning, ARP/NDP learning, and IEEE802.1X authentication when a free space is provided in the MAC address table.
2. Clear the executed command (for No. 2, 3, 4 and 6 in the above table).
3. Make a free space in the MAC address table.*
4. Re-execute the command (for No. 2, 3, 4 and 6 in the above table) or re-authenticate (for No. 5).

* To provide a free space in the MAC address table, registered entries must be cleared. The clear procedure for each entry is shown in the table below.

Table 4-3: Operation Log Message for Checking Resource Use Status

No.	File Name Specified for "get"	Log Message
1	Learned MAC addresses	Execute the <code>clear mac-address-table</code> command and the <code>clear arp-cache</code> command.* ¹
2	Static MAC address Static ARP/NDP MAC address learning suppression function	Execute the configuration command below to clear the configuration.* ² -no mac-address-table static -no arp -no ipv6 neighbor -mac-address table learning vlan
3	IEEE802.1X	Execute the <code>clear dot1x auth-state</code> command to reset authentication.* ¹
4	MAC address for Ring Protocol	- Execute the configuration command <code>disable</code> to disable Ring Protocol.* ² - Execute any of the configuration commands below to clear the configuration.* ² -no axrp -no axrp vlan-mapping -no axrp-ring-port -no control-vlan -no mode -no vlan-group
5	IGMP/MLD Snooping	Execute the <code>clear igmp-snooping all</code> command or the <code>clear mld-snooping all</code> command.* ¹
6	Web authentication	Execute the <code>clear web-authentication auth-state</code> command to reset authentication.* ¹
7	MAC authentication	Execute the <code>clear mac-authentication auth-state</code> command to reset authentication.* ¹

4. Troubleshooting Communication Failures Due to Resource Shortage [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]

*1 For details, see the manual "Operation Commands."

*2 For details, see the manual "Configuration Commands."

4.2 When Resource Shortage of VLAN Identification Table Occurs

4.2.1 Checking VLAN Identification Table Resource Usage

This system outputs an operation log message when the usage of VLAN identification table reaches 80% of the accommodating condition. The operation log message to be output is shown in the table below.

Table 4-4: Operation Log Message for Checking Resource Usage

No.	Trigger	Log Message
1	When VLAN identification table use status reaches 80%	VLAN classification table entries was beyond 80 percent of capacity.

Communication is not immediately affected when the system reached usage of 80%. However, if the VLAN identification table is continuously used by L2 authentication function or the like, the limit of the accommodating condition may be reached and resource shortage disabling authentication by the L2 authentication function may arise. Check the set value and accommodation value in advance so that the limit of the accommodating condition will not be exceeded.

Check the usage of the VLAN identification table by referring to the manual "Configuration Settings."

4.2.2 Action to Be Taken When VLAN Identification Table Resource Shortage Occurs

When usage of VLAN identification table reaches the limit of the accommodating condition, the corresponding log message is output at the timing listed in the table below.

Table 4-5: Operation Log Message for Checking Resource Use Status

No.	Trigger	Log Message
1	Setting tag translation function	- The vlan mapping entry can't be registered at VLAN classification table (VLAN <ID>, port(<NIF No.>/<Port No.>)). - The vlan mapping entry can't be registered at VLAN classification table (VLAN <ID>, Channel Group <Channel Group Number>).
2	Setting protocol VLAN	- The protocol based VLAN entry can't be registered at VLAN classification table (VLAN <ID>,port(<NIF No.>/<Port No.>)). - The protocol based VLAN entry can't be registered at VLAN classification table (VLAN <ID>,Channel Group <Channel Group Number>). - The protocol based VLAN entry can't be registered at VLAN classification table (protocol {ethertype llc snap-ethertype }<HEX>,VLAN <ID>). - The protocol based VLAN entry can't be registered at VLAN classification table (protocol {ethertype llc snap-ethertype }<HEX>,Vlan-Protocol <Protocol name>).
3	Setting MAC VLAN static entry	- The MAC-VLAN MAC Address entry can't be registered at hardware tables.
4	IEEE802.1X authentication (VLAN authentication (dynamic))	- The 802.1X Supplicant MAC address of MAC VLAN can't be registered at hardware tables. Note: This log is displayed when the <code>show dot1x logging</code> command is executed.
5	Authentication VLAN	- The registration of the MAC address failed. Note: This log is displayed when the <code>show fense logging</code> command is executed.
6	Web Authentication (Dynamic VLAN mode)	- The login failed because of hardware restriction. Note: This log is displayed when the <code>show web-authentication logging</code> command is executed.

If these log messages are output, the function that newly uses the VLAN identification address table cannot be set. Review the network configuration and set the configuration allowing for operation below the limit of the system's accommodating condition.

No. 1, 2, and 3 in the above table show that setting cannot be registered to the VLAN identification table by the configuration command. No. 4 and 5 show that setting cannot be registered to the VLAN identification table. For re-setting, follow the steps below.

1. Review the configuration so that new entries will not be registered by IEEE802.1X authentication, Web authentication, and authentication VLAN when a free space is provided in the VLAN identification table.
2. Clear the executed command (for No. 1, 2, and 3 in the above table).
3. Make a free space in the VLAN identification table.*
4. Re-execute the command (for No. 1, 2, and 3 in the above table), or re-authenticate (for No. 4), or review the number of users to be authenticated by the authentication server (for No. 5).

* To provide a free space in the VLAN identification table, registered entries must be cleared. The clear procedure for each entry is shown in the table below.

Table 4-6: VLAN Identification Table Entry Clear Method

No.	Entry to Be Cleared	Step
1	Tag translation function	Execute configuration command <code>no switchport vlan mapping enable and no switchport vlan mapping.</code> *1
2	Protocol VLAN	Execute configuration command <code>no switchport protocol</code> to clear the protocol VLAN setting.*1
3	MAC VLAN static entry	Execute configuration command <code>"no mac-address."</code> *1
4	IEEE802.1X authentication	Execute <code>"clear dot1x auth-state"</code> command.*2
5	Authentication VLAN	Review the number of users to be authenticated by the authentication server.
6	Web Authentication	Execute the <code>clear web-authentication auth-state</code> command.

*1 For details, see the manual "Configuration Commands."

*2 For details, see the manual "Operation Commands."

4.3 When Resource Shortage Occurs in Shared Memory

4.3.1 Checking Resource Usage of Shared Memory

Shared memory usage can be checked with the `show system` command.

```
# show system
:
Shared resources Used/Max: 0B/1638400B
  IPv4 Unicast Single-path used : 0B
  IPv4 Unicast Multi-path used : 0B
  IPv6 Unicast Single-path used : 0B
  IPv6 Unicast Multi-path used : 0B
  IPv4 Multicast used : 0B
  IPv6 Multicast used : 0B
  IPv4 Policy Based Routing used: 0B
  IPv6 Policy Based Routing used: 0B
  VLAN config used : 0B
  IGMP/MLD Snooping used : 0B
:
```

For details of the `show system` command, see the manual "Operation Commands."

4.3.2 Action to Be Taken When Resource Shortage of Shared Memory Occurs

When resource shortage of shared memory occurs, see the manual "Configuration Settings" to check the set value and accommodation value.

5

Collecting Failure Information

This chapter focuses on collecting the failure information.

[5.1 Collecting Failure Information](#)

[5.2 Transferring Files for Maintenance Information](#)

[5.3 Writing to MC](#)

5.1 Collecting Failure Information

The information on failures can be collected at once using the `show tech-support` command. This command can also transfer the collected failure information to a specified ftp server (see "[5.2.3 Transferring Maintenance Information Files Using show tech-support Command](#)").

Memory dump at failure occurrence time can be collected by using the `dump` command.

5.1.1 Collecting Failure Information Using ftp Command from the Operation Terminal

(1) Acquire failure information from the remote operation terminal

Table 5-1: Available Information via "ftp"

No.	File Name Specified for "get"	Acquiring Basic Information
1	<code>.show-tech</code>	Result of <code>show tech-support</code>
2	<code>.show-tech-unicast</code>	Result of <code>show tech-support unicast</code>
3	<code>.show-tech-multicast</code>	Result of <code>show tech-support multicast</code>
4	<code>.show-tech-layer-2</code>	Result of <code>show tech-support layer-2</code>

Figure 5-1: Collecting Failure Information from the Remote Operation Terminal

Collecting basic information

```

client-host> ftp 192.168.0.60 <----- 1
Connected to 192.168.0.60.
220 192.168.0.60 FTP server (NetBSD-ftpd) ready.
Name (192.168.0.60:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get .show-tech show-tech.txt <----- 2
local: show-tech.txt remote: .show-tech
150 Opening BINARY mode data connection for '/etc/ftpshowtech'.
226 Transfer complete.
270513 bytes received in 8.22 seconds (32.12 KB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.60.
client-host>

```

"show-tech.txt" file is transferred to the client host.

Collecting unicast information

```

client-host> ftp 192.168.0.60 <----- 3
Connected to 192.168.0.60.
220 192.168.0.60 FTP server (NetBSD-ftpd) ready.
Name (192.168.0.60:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get .show-tech-unicast show-tech-uni.txt <----- 4
local: show-tech-uni.txt remote: .show-tech-uni.txt
150 Opening BINARY mode data connection for '/etc/ftpshowtech'.
226 Transfer complete.
343044 bytes received in 30.43 seconds (11.01 KB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.60.
client-host>

```

"show-tech-uni.txt" file is transferred to the client host.

1. Connected from ftp client to system via ftp
2. Transfer .show-tech file
3. Connected from ftp client to system via ftp
4. File transfer

Note

- Because ftp-related commands such as `ls` command cannot show any file to be obtained, the file sizes cannot be determined in advance.
- Fetching the information takes a long time because the command is processed on the system. However, do not cancel the process on the way.
- The loading state of the system or condition of the communication path might cause a network timeout, which makes the client disconnect a line. In this case, set a longer period of time for the client timeout.
- Failure information obtained via ftp does not contain the results of executing the system administrator commands such as `show running-config` command.
- Executing the `show tech-support` command records "ftpuser" as a user name in the log information.

5.1.2 Collecting Failure Information Using dump Command [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]

(1) Collecting memory dump when communication failure occurs

When any communication failure occurs, collect memory dump by executing all of the following commands. The collected memory dump files are stored under /dump0 in the system where the command is executed. Delete the memory dump file after collecting it.

For IP8800/S6700

1. Execute the `dump bsu` command for all installed BSUs from the active BCU.
2. Execute the `dump nif` command for all faulty ports from the active BCU.

[Example]

The following is an example when communication failure occurs in NIF number 1 and port number 1 in the case that BSUs are installed in BSU number 1 and 2.

1. Login the active BCU and execute the dump command.


```
> dump bsu 1
Dump command accept.
>
11/01 17:43:42 E3 BSU BSU:1 25070700 1681:000000000000 BSU online dump command
executed.
```
2. After above log is displayed, execute next dump command.


```
> dump bsu 2
Dump command accept.
>
11/01 18:10:42 E3 BSU BSU:2 25070700 1681:000000000000 BSU online dump command
executed.
```
3. After above log is displayed, execute next dump command.


```
> dump nif 1
Dump command accept.
>
11/01 18:15:42 E3 NIF NIF:1 25000700 1240:000000000000 NIF online dump command
executed.
```

For IP8800/S6600

1. Execute the `dump psp` command for all installed PSPs from the active system.
2. Execute the `dump nif` command for all faulty ports from the active system.

[Example]

The following is an example when communication failure occurs in NIF number 1 and port number 1 in the case that BSUs are installed in BSU number 1 and 2.

1. Login the active system and execute the dump command.


```
> dump psp
psp command accept.
>
11/01 17:43:42 E3 CSU 25070700 2301:000000000000 PSP online dump command
executed.
```
2. After above log is displayed, execute next dump command.


```
> dump nif 1
Dump command accept.
>
11/01 18:10:42 E3 NIF NIF:1 25000700 1240:000000000000 NIF online dump command
executed.
```

For IP8800/S6300

1. Execute the `dump psp` command for the active PSP from the active system.

- Execute the `dump nif` command for the faulty port from the active system.

[Example]

The following is an example when communication failure occurs in NIF number 1 and port number 1.

- Login the active system and execute the `dump` command.

```
> dump psp
Dump command accept.
>
11/01 17:43:42 E3 MSU 25070700 2301:000000000000 PSP online dump command
executed.
```

- After above log is displayed, execute next `dump` command.

```
> dump nif 1
Dump command accept.
>
11/01 18:10:42 E3 NIF NIF:1 25000700 1240:000000000000 NIF online dump command
executed.
```

(2) Collecting memory dump when communication failure occurs after switchover of BCU [IP8800/S6700], CSU [IP8800/S6600], and MSU [IP8800/S6300]

When any communication failure occurs after switchover, collect memory dump by executing all of the following commands. The collected memory dump files are stored under "/dump0" in the system where the command is executed. Delete the memory dump file after collecting it.

For IP8800/S6700

- Execute the `dump bsu` command for all installed BSUs from the active BCU.
- Execute the `dump nif` command for all faulty ports from the active BCU.
- Execute the `dump bsu` command for any one of installed BSUs from the standby BCU. No need to execute the command for any BSU.

[Example]

The following is an example when communication failure occurs in NIF number 1 and port number 1 on condition that BCUs are installed in BSU number 1 and 2 as redundant configuration.

- Login the active BCU and execute the `dump` command.

```
> dump bsu 1
Dump command accept.
>
11/01 17:43:42 E3 BSU BSU:1 25070700 1681:000000000000 BSU online dump command
executed.
```

- After above log is displayed, execute next the `dump` command.

```
> dump bsu 2
Dump command accept.
>
11/01 18:10:42 E3 BSU BSU:2 25070700 1681:000000000000 BSU online dump command
executed.
```

- After above log is displayed, execute next `dump` command.

```
> dump nif 1
Dump command accept.
>
11/01 18:15:42 E3 NIF NIF:1 25000700 1240:000000000000 NIF online dump command
executed.
```

- After above log is displayed, log in the standby BCU and execute next `dump` command.

```
SBY:> dump bsu 1
Dump command accept.
SBY:>
11/01 18:17:42 E3 BSU BSU:1 25070700 1681:000000000000 BSU online dump command
executed.
```

5. Collecting Failure Information

For IP8800/S6600

1. Execute the `dump psp` command for active PSP from the active system.
2. Execute the `dump nif` command for all faulty ports from the active system.
3. Execute the `dump psp standby` command for the standby PSP from the active system.
4. Execute the `dump psp` command for the standby PSP from the active system.

[Example]

The following is an example when communication failure occurs in NIF number 1 and port number 1 on condition that CSU is in redundant configuration.

1. Log in the active system and execute the `dump` command.

```
> dump psp
Dump command accept.
>
11/01 17:43:42 E3 CSU 25070700 2301:000000000000 PSP online dump command
executed.
```

2. After above log is displayed, execute next `dump` command.

```
> dump nif 1
Dump command accept.
>
After above log is displayed, execute next the dump command.
> dump bsu 2
Dump command accept.
>
11/01 18:10:42 E3 BSU BSU:2 25070700 1681:000000000000 BSU online dump command
executed.
```

3. After above log is displayed, execute next `dump` command.

```
> dump psp standby
Dump command accept.
>
11/01 18:18:42 E3 CSU 25070700 2301:000000000000 PSP online dump command
executed.
```

4. After above log is displayed, execute next `dump` command.

```
> dump psp
Dump command accept.
>
11/01 18:20:42 E3 CSU 25070700 2301:000000000000 PSP online dump command
executed.
```

For IP8800/S6300

1. Execute the `dump psp` command for the active PSP from the active system.
2. Execute the `dump nif` command for the faulty port from the active system.
3. Execute the `dump psp standby` command for the standby PSP from the active system.
4. Execute the `dump psp` command for the standby PSP from the standby system.

[Example]

The following is an example when communication failure occurs in NIF number 1 and port number 1 in case that MSU is in redundant configuration.

1. Login the active system and execute the `dump` command.

```
> dump psp
Dump command accept.
>
11/01 17:43:42 E3 MSU 25070700 2301:000000000000 PSP online dump command
executed.
```

2. After above log is displayed, execute next `dump` command.

```
> dump nif 1
Dump command accept.
>
11/01 18:15:42 E3 NIF NIF:1 25000700 1240:000000000000 NIF online dump command
executed.
```

3. After above log is displayed, execute next dump command.

```
> dump psp standby
Dump command accept.
>
11/01 18:18:42 E3 MSU 25070700 2301:000000000000 PSP online dump command
executed.
```

4. After above log is displayed, login the standby system and execute next dump command.

```
SBY:> dump psp
Dump command accept.
SBY:>
11/01 18:20:42 E3 MSU 25070700 2301:000000000000 PSP online dump command
executed.
```

(3) Collecting memory dump when communication failure occurs after switchover of BSU [IP8800/S6700]

When any communication failure occurs after switchover of BSU, collect memory dump by executing all of the following commands. The collected memory dump files are stored under `/usr/var/hardware` (In Ver.10.5 or earlier, `/dump0`) in the system where the command is executed. Delete the memory dump file after collecting them.

1. Execute the `dump bsu` command for all installed BSUs from the active BCU.
2. Execute the `dump nif` command for all faulty ports from the active BCU.

[Example]

The following is an example when communication failure occurs in NIF number 1 and port number 1 on condition that BSUs are installed in BSU number 1 and 2.

1. Log in the active BCU and execute the dump command.

```
> dump bsu 1
Dump command accept.
>
11/01 17:43:42 E3 BSU BSU:1 25070700 1681:000000000000 BSU online dump command
executed.
```

2. After above log is displayed, execute next dump command.

```
> dump bsu 2
Dump command accept.
>
11/01 18:10:42 E3 BSU BSU:2 25070700 1681:000000000000 BSU online dump command
executed.
```

3. After above log is displayed, execute next dump command.

```
> dump nif 1
Dump command accept.
>
11/01 18:15:42 E3 NIF NIF:1 25000700 1240:000000000000 NIF online dump command
executed.
```

5.2 Transferring Files for Maintenance Information

This section describes how to transfer log information or dump information automatically stored when failure occurred while operating to the console or remote operation terminal. Three commands are available, that is, `ftp`, `zmodem` **[IP8800/S3600]** **[IP8800/S2400]**, and `show tech-support`. Maintenance information includes the following items.

Table 5-2: Maintenance Information

No.	Item	Storage Location and File Name	File Transfer Format for ftp Command
1	Dump information file created when system restarts	<code>/dump0/rmdump</code> Delete the file after transfer.	binary
2	Dump information file created when BSU failure occurs [IP8800/S6700]	<code>/usr/var/hardware/bsu**.*</code> in the active or standby system where the failure occurs (In Ver.10.5 or earlier, <code>/dump0/bsu**.*</code>) ** : BSU number of the faulty BSU *** : Serial number assigned from when dump was collected. Up to two files, oldest and latest files, are stored. Delete the file after transfer.	binary
3	BSU dump information file created when the <code>dump bsu</code> command is executed [IP8800/S6700]	<code>/dump0/bsu**.cmd</code> in the active or standby system where the command is executed ** : BSU number of the specified BSU Delete the file after transfer.	binary
4	Dump information file created when PSP failure occurs [IP8800/S6300]	<ul style="list-style-type: none"> <code>/usr/var/hardware/psp**.*</code> in the active or standby system where the failure occurs (In Ver.10.5 or earlier, <code>/dump0/psp**.*</code>) (The information is stored in above location in the active system even if the failure occurred in the standby PSP. Confirm whether dump information was collected in the active or standby system according to the file name.) ** : If PSP where the failure occurred is MSU1, 01 is indicated. If PSP where the failure occurred is MSU2, 02 is indicated. *** : Serial number assigned from when dump was collected. Up to two files, the oldest and latest files are stored. <code>/dump0/rmdump</code> in the system where the failure occurs (The information is collected simultaneously. If the failure occurred in the standby PSP, it is collected in the standby system.) Delete the file after transfer. 	binary
5	PSP dump information file created when the <code>dump psp</code> command is executed [IP8800/S6300]	<code>/usr/var/hardware/psp**.*</code> in the active or standby system where the command is executed (In Ver.10.5 or earlier, <code>/dump0/psp**.cmd</code>) ** : If specified PSP is MSU1, 01 is indicated. If specified PSP is MSU2, 02 is indicated. Confirm whether dump information was collected in the active or standby system according to the file name. *** : Serial number assigned from when dump was collected. Up to two files, the oldest and latest files are stored. Delete the file after transfer.	binary
6	Dump information file created when NIF failure occurs [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]	<code>/usr/var/hardware/nif**.*</code> in the active system (In Ver.10.5 or earlier, <code>/dump0/nif**.*</code>) ** : NIF number of the faulty NIF *** : Serial number assigned from when dump was collected. Up to two files, the oldest and latest files, are stored. Delete the file after transfer.	binary

No.	Item	Storage Location and File Name	File Transfer Format for ftp Command
7	NIF dump information file created when the dump nif command is executed [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]	/usr/var/hardware/nif**.* in the active or standby system where the command is executed (In Ver.10.5 or earlier, /dump0/nif**.*cmd) ** : NIF number of the specified NIF *** : Serial number assigned from when dump was collected. Up to two files, the oldest and latest files, are stored. Delete the file after transfer.	binary
8	Dump information file created when network interface failure occurs [IP8800/S3600] [IP8800/S2400]	/usr/var/hardware/ni**.* (In Ver10.5 or earlier, /dump0/ni**.**) * : 0 to 9 *** : Serial number assigned from when dump was collected. Up to two files, the oldest and latest files, are stored. Delete the files after transfer.	binary
9	Log information	Stored with the following name depending on the collected directory (see "Figure 5-3: Transferring Log Information Files to the Remote Operation Terminal"). Operation log: log.txt Type log: log_ref.txt	ASCII
10	Configuration file created when failure occurs	Using system administrator mode, perform the following command and copy two files to home directory, then transfer the files. cp /config/system.cnf system.cnf cp /config/system.txt system.txt Delete the files after transfer.	binary
11	Information saved upon occurrence of a failure	/usr/var/core/*.core Delete the file after transfer.	binary

5.2.1 Transferring Files Using ftp Command

Use the ftp command to transfer files between this system and the remote operation terminal.

(1) Transferring dump files to the remote operation terminal

Figure 5-2: Transferring Dump Files to the Remote Operation Terminal

```

> cd <dump-stored directory> <-----1
> ftp 192.168.0.1 <-----2
Connected to 192.168.0.1.
220 FTP server (Version 6.00LS) ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> prompt <-----3
Interactive mode off.
ftp> bin <-----4
200 Type set to I.
ftp>cd <target directory> <-----5
250 CMD command successful.
ftp> put <dump file name> <-----6
local: <dump file name> remote: <dump file name>
200 EPRT command successful.
150 Opening BINARY mode data connection for '<dump file name>'.
100% |*****| 3897 2.13 MB/s 00:00 ETA
226 Transfer complete.
3897 bytes sent in 00:00 (82.95 KB/s)
ftp> bye
221 Goodbye.
>

```

1. Specify the directory where the dump files to be transferred are located.

5. Collecting Failure Information

2. Specify the address of target.
3. Changes the interaction mode.
4. Enter binary mode.*
5. Specify the target directory.
6. Transfers the dump file.

*

Be sure to transfer dump files in binary mode. The correct dump information will not be obtained if dump files are transferred in ASCII mode.

(2) Transferring log information to the remote operation terminal

Figure 5-3: Transferring Log Information Files to the Remote Operation Terminal

```
> show logging > log.txt
> show logging reference > log_ref.txt
> ftp 192.168.0.1 <-----1
Connected to 192.168.0.1.
220 FTP server (Version 6.00LS) ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ascii <-----2
200 Type set to A.
ftp>cd <target directory> <-----3
250 CMD command successful.
ftp> put log.txt <-----4
local: log.txt remote: log.txt
200 EPRT command successful.
150 Opening ASCII mode data connection for 'log.txt'.
100% |*****| 89019 807.09 KB/s --:-- ETA
226 Transfer complete.
89019 bytes sent in 00:00 (315.22 KB/s)
ftp> put log_ref.txt
local: log_ref.txt remote: log_ref.txt
200 EPRT command successful.
150 Opening ASCII mode data connection for 'log_ref.txt'.
100% |*****| 4628 1.04 MB/s --:-- ETA
226 Transfer complete.
4628 bytes sent in 00:00 (102.86 KB/s)
ftp> bye
221 Goodbye.
>
```

1. Specify the address of target.
2. Set to the ASCII mode.
3. Specify the target directory.
4. Transfer the log information.

(3) Transferring failure backup information files to the remote operation terminal**Figure 5-4: Transferring the Failure Backup Information File to the Remote Operation Terminal**

```

> cd /usr/var/core/
> ls <-----1
nimd.core      nodeInit.core
> ftp 192.168.0.1 <-----2
Connected to 192.168.0.1.
220 FTP server (Version 6.00LS) ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> prompt <-----3
Interactive mode off.
ftp> bin <-----4
200 Type set to I.
ftp>cd <target directory> <-----5
250 CMD command successful.
ftp> mput *.core <-----6
local: nimd.core remote: nimd.core
200 EPRT command successful.
150 Opening BINARY mode data connection for 'nimd.core'.
100% |*****|
272 KB 1.12 MB/s 00:00 ETA
226 Transfer complete.
278528 bytes sent in 00:00 (884.85 KB/s)
local: nodeInit.core remote: nodeInit.core
200 EPRT command successful.
150 Opening BINARY mode data connection for 'nodeInit.core'.
100% |*****|
1476 KB 1.40 MB/s 00:00 ETA
226 Transfer complete.
1511424 bytes sent in 00:01 (1.33 MB/s)
ftp> bye
221 Goodbye.
>

```

1. Check if the failure backup information file exists. If no file exists, exit without any action.
2. Specify the target terminal address.
3. Change the interaction mode.
4. Enter binary mode.*
5. Specify a transfer target directory.
6. Transfer the failure backup information file.

*

Be sure to transfer the failure backup information file in binary mode. The accurate information will not be obtained if the failure backup information file is transferred in ASCII mode.

5.2.2 Transferring Files Using zmodem Command [IP8800/S3600] [IP8800/S2400]

To transfer files between this system and the console connected via RS232C cable, the `zmodem` command is used. Before starting communication, prepare the communication program on the console for receiving.

(1) Transferring dump files to a console

Figure 5-5: Transferring Dump Files to a Console

```
> cd <dump-stored directory>          <-----1
> zmodem put rmdump                    <-----2
>
```

1. Specify a directory where the dump files to be transferred is located.
2. Transfer the dump file.

(2) Transferring log information to a console

Figure 5-6: Transferring Log Files to a Console

```
> show logging > log.txt
> show logging reference > log_ref.txt
> zmodem put log.txt                  <-----1
> zmodem put log_ref.txt
>
```

1. Transfer the log file.

(3) Transferring failure backup information files to a console

Figure 5-7: Transferring Failure Backup Information Files to a Console

```
> cd /usr/var/core/
> ls                                  <-----1
interfaceControl.core  nodeInit.core
> zmodem put interfaceControl.core    <-----2
> zmodem put nodeInit.core
>
```

1. Check if the failure backup information file exists. If no file exists, exit without any action.
2. Transfer log files.

5.2.3 Transferring Maintenance Information Files Using show tech-support Command

Use the `show tech-support` command when transferring maintenance information files to the remote operation terminal or remote host.

(1) Transferring maintenance information to the remote operation terminal or remote host

Figure 5-8: Transferring Maintenance Information Files to the Remote Operation Terminal or Remote Host
[IP8800/S6700] [IP8800/S6600] [IP8800/S6300]

```

> show tech-support ftp <---1
Specify Host Name of FTP Server.      : 192.168.0.1 <---2
Specify User ID for FTP connections.  : staff1 <---3
Specify Password for FTP connections. : <---4
Specify Path Name on FTP Server.      : /usr/home/staff1 <---5
Specify File Name of log and Dump files: support <---6
Check and Extract Dump Files in a Standby system?(y/n)y <---7
Mon Dec 18 21:49:59 UTC 2006
Transferred support.txt .
Executing.
.....
.....
.....
Operation normal end.
##### Dump files' Information #####
**** ls -l /dump0 ****
total 4568
-rwxrwxrwx 1 root wheel 4677464 Dec 18 21:16 rmdump
**** ls -l /usr/var/hardware ****
-rwxrwxrwx 1 root wheel 130886 Dec 8 16:43 nif01.000
**** ls -l /standby/dump0 ****
total 0
-rwxrwxrwx 1 root wheel 4207084 Dec 18 21:16 rmdump
**** ls -l /standby/usr/var/hardware ****
##### End of Dump files' Information #####
##### Core files' Information #####
**** ls -l /usr/var/core ****
**** ls -l /standby/usr/var/core ****
No Core files
##### End of Core files' Information #####
Transferred support.tgz .
Executing.
.....
.....
.....
Operation normal end.
>

```

1. Execute command.
2. Specify the remote host name.
3. Specify a user name.
4. Enter a password.
5. Specify a transfer target directory.
6. Specify a file name.
7. Select whether to collect dump files of standby system.

Figure 5-9: Transferring Maintenance Information Files to the Remote Operation Terminal or Remote Host
[IP8800/S3600] [IP8800/S2400]

```

> show tech-support ftp <---1
Specify Host Name of FTP Server.      : 192.168.0.1 <---2
Specify User ID for FTP connections.  : staff1 <---3
Specify Password for FTP connections. : <---4
Specify Path Name on FTP Server.      : /usr/home/staff1 <---5
Specify File Name of log and Dump files: support <---6
Mon Dec 18 20:42:58 UTC 2006
Transferred support.txt .
Executing.
.....

```

5. Collecting Failure Information

```

.....
.....
.....
Operation normal end.
##### Dump files' Information #####
**** ls -l /dump0 ****
total 2344
-rwxrwxrwx 1 root wheel 2400114 Dec 8 16:46 rmdump
**** ls -l /usr/var/hardware ****
-rwxrwxrwx 1 root wheel 264198 Dec 8 16:43 ni00.000
##### End of Dump files' Information #####
##### Core files' Information #####
**** ls -l /usr/var/core ****
No Core files
##### End of Core files' Information #####
Transferred support.tgz .
Executing.
.....
.....
.....
Operation normal end.
>

```

1. Execute command.
2. Specify the remote host name.
3. Specify a user name.
4. Enter a password.
5. Specify a transfer target directory.
6. Specify a file name.

5.2.4 Transferring Files Using ftp Command from the Operation Terminal

(1) Collecting dump information files from the remote operation terminal

Table 5-3: Files That Can Be Acquired Using ftp Command

No.	File Name Specified for "get"	Acquired Files
1	.dump	Files under /dump0 and /usr/var/hardware (compressed) (In Ver.10.5 or earlier, files under /dump0 and /dump1 (compressed))
2	.dump0	Files under /dump0 (compressed)
3	.hardware	Files under /usr/var/hardware (compressed) (Ver.10.5 or later)

Figure 5-10: Collecting Dump Files from the Remote Terminal

```

client-host> ftp 192.168.0.60 <---1
Connected to 192.168.0.60.
220 192.168.0.60 FTP server (NetBSD-ftp) ready.
Name (192.168.0.60:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary <---2
200 Type set to I.
ftp> get <file name> dump.tgz <---3
local: dump.tgz remote: .dump
150 Opening BINARY mode data connection for '/etc/ftpdump'.
226 Transfer complete.
2411332 bytes received in 5.78 seconds (407.13 KB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.60.
client-host>

```

dump.tgz files are acquired by client host.

1. The ftp client is connected to the system via ftp.
2. Be sure to transfer the dump information files in binary mode. Files cannot be transferred in ASCII mode.
3. Transfer dump files.

Note

- Because ftp-related commands such as ls command cannot show any file to be obtained, the file sizes cannot be determined in advance.
- The loading state of the system or condition of the communication path might cause a network timeout, which makes the client disconnect a line. In this case, set a longer period of time for the client timeout.

5.3 Writing to MC

The failure and maintenance information can be written to MC. Note that MC is subject to the capacity limit.

5.3.1 Writing File to MC Using Operation Terminal

When writing the system information to MC, use the operation terminal.

Figure 5-11: Writing Information to MC

Insert MC to which the information is written.

Check the size of the file to be copied (tech.log) using the `ls -l` command.)

```
> ls -l tech.log
-rw-r--r--  1 operator  users  234803 Nov 15 15:52 tech.log
```

Check the free space using the `show mc` command.

```
>show mc
Date 2005/11/15 15:50:40 UTC
MC  : Enabled
      Manufacture ID : 00000003
      16,735kB used
      106,224kB free   <----- 1
      122,959kB total
```

Copy the source file to MC with name "tech-1.log" by using the `cp` command.

```
> cp tech.log mc-file tech-1.log
```

Verify that the file has been written to MC.

```
> ls mc-dir
Name          Size
tech-1.log    234803
>
```

1. Free space

6

Line Test

[6.1 Testing Line](#)

6.1 Testing Line

6.1.1 Ethernet Port

In line tests, the loopback points of frames or data sent for the test differs depending on the type of test specified. The frame loopback points for each test type is given in the figure below:

Figure 6-1: Loopback Points of Frames for Each Type of Line Test

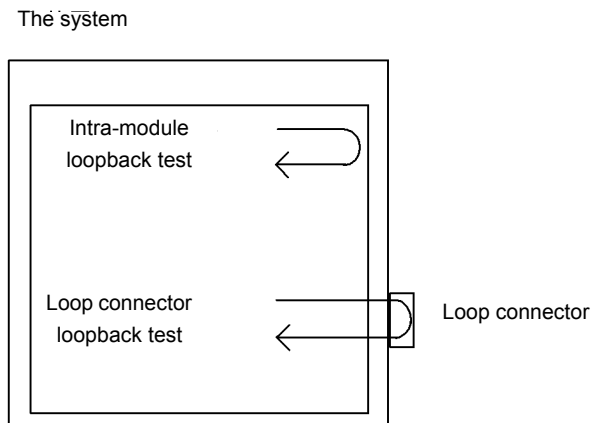


Table 6-1: Line Test Type for Each Frame Loopback Point

Frame Loopback Point	Line Test Type	Failure That Can Be Identified
System	Intra-module loopback test	System (excluding RJ45 connectors or transceiver)
Loop connector	Loop connector loopback test	System (including RJ45 connectors and transceiver)

In addition, executable test types also differ depending on the type of line. For the line types and available test types, see the manual "Operation Commands."

The following is an explanation of test methods for each type of test.

(1) Checking frame loopback within system

When checking the frame loopback in the system, perform the intra-module loopback test. Use the `inactivate` command to set the port to inactive state before executing the intra-module loopback test. To end the test, use the `activate` command to change the port from inactive to active. In this test, test frame loops back in this system to check for the NIF failure **[IP8800/S6700]** **[IP8800/S6600]** **[IP8800/S6300]** and system failure (excluding RJ45 connector and transceivers) **[IP8800/3600]** **[IP8800/S2400]**.

This test is available for all line types.

IP8800/S6700, IP8800/S6600, and IP8800/S6300

A case of test conducted on Port 1 of NIF 1 at a transmission interval of one second is shown as a test example. Execute the `test interfaces` command and the `no test interfaces` command in this order from the operation terminal.

```
> inactivate gigabitethernet 1/1 [Enter]
> test interfaces gigabitethernet 1/1 internal [Enter]
```

(Wait about 1 minute.)


```
> no test interfaces gigabitethernet 1/1 [Enter]
> activate gigabitethernet 1/1 [Enter]
```

IP8800/S3600 and IP8800/S2400

A case of test conducted on Port 1 of NIF 0 at a transmission interval of one second is shown as a test example. Execute the `test interfaces` command and the `no test interfaces` command in this order from the operation terminal.

```
> inactivate gigabitethernet 0/1 [Enter]
> test interfaces gigabitethernet 0/1 internal [Enter]
```

(Wait about 1 minute.)

```
> no test interfaces gigabitethernet 0/1 [Enter]
> activate gigabitethernet 0/1 [Enter]
```

As the command execution result, the screens shown in "[Figure 6-2: Execution Result Example of the test interfaces command and the no test interfaces command \[IP8800/S6700\] \[IP8800/S6600\] \[IP8800/S6300\]](#)," the `no test interfaces` command [\[IP8800/S6700\] \[IP8800/S6600\] \[IP8800/S3600\]](#), "[Figure 6-3: Execution Result Example of the test interfaces command and the no test interfaces command \[IP8800/S3600\] \[IP8800/S2400\]](#)," and the `no test interfaces` Command [\[IP8800/S3600\] \[IP8800/2400\]](#) are displayed. Check the following:

"Send-NG" and "Receive-NG" are 0.

If "Send-NG" and "Receive-NG" are 0, the line test result is acceptable.

If "Send-NG" and "Receive-NG" are not 0, some abnormality exists. See the display contents of the line test execution result in the manual "Operation Commands."

If "Send-NG" and "Receive-NG" are not 0 for 10GBASE-R, re-execute the line test and check if "Send-NG" and "Receive-NG" are 0. If "Send-NG" and "Receive-NG" are not 0, some abnormality exists. See the display contents of the line test execution result in the manual "Operation Commands."

Figure 6-2: Execution Result Example of the test interfaces command and the no test interfaces command [IP8800/S6700] [IP8800/S6600] [IP8800/S6300]

```
> inactivate gigabitethernet 1/1
> test interfaces gigabitethernet 1/1 internal interval 2 pattern 4

> no test interfaces gigabitethernet 1/1
> activate gigabitethernet 1/1
Date 2006/03/10 00:20:21 UTC
Interface type          :100BASE-TX
Test count              :12
Send-OK                 :12                Send-NG                :0
Receive-OK              :12                Receive-NG             :0
Data compare error      :0                 Out underrun           :0
Out buffer hunt error   :0                 Out line error         :0
In CRC error            :0                 In frame alignment     :0
In monitor time out    :0                 In line error          :0
H/W error               :none
```

Figure 6-3: Execution Result Example of the `test interfaces` command and the `no test interfaces` command [IP8800/S3600] [IP8800/S2400]

```
> deactivate gigabitethernet 0/1
> test interfaces gigabitethernet 0/1 internal interval 2 pattern 4

> no test interfaces gigabitethernet 0/1
> activate gigabitethernet 0/1
Date 2005/11/10 00:20:21 UTC
Interface type      :100BASE-TX
Test count         :12
Send-OK            :12                Send-NG                :0
Receive-OK         :12                Receive-NG             :0
Data compare error :0
Out buffer hunt error :0                Out line error        :0
In CRC error       :0                In frame alignment    :0
In monitor time out :0                In line error         :0
H/W error          :none
```

(2) Checking frame loopback at a loop connector

Execute the loop connector loopback test to check frame loopback at a loop connector. Before performing loop connector loopback test or connecting the loop connector, use the `inactivate` command to set the port in the inactive state. To end the test, restore the connection and use the `activate` command to change the port from inactive to active. In this test, test frame loops back at a loop connector connected to this system to check for the NIF failure [IP8800/S6700] [IP8800/S6600] [IP8800/S6300] and system failure (including RJ45 connector and transceivers) [IP8800/S3600] [IP8800/S2400]. This test is available for all line types.

For each line type, remove the cable of the test target port number and connect the loop connector for each line type to execute the test. Note that, if the loop connector is not connected or the appropriate loop connector for the port is not connected, the test cannot be successfully executed.

IP8800/S6700, IP8800/S6600, and IP8800/S6300

A case of test conducted on Port 1 of NIF 1 at a transmission interval of one second after the cable is removed and the loop connector for each line type is connected is shown as a test example.

Execute the `test interfaces` command and the `no test interfaces` command in this order from the operation terminal.

```
> deactivate gigabitethernet 1/1 [Enter]
```

(Connect the loop connector to the corresponding port.)

```
> test interfaces gigabitethernet 1/1 connector [Enter]
```

(Wait about 1 minute.)

```
> no test interfaces gigabitethernet 1/1 [Enter]
```

(Remove the loop connector from the corresponding port and restore the connection.)

```
> activate gigabitethernet 1/1 [Enter]
```

IP8800/S3600 and IP8800/S2400

A case of test conducted on Port 1 of NIF 0 at a transmission interval of one second after the cable is removed and the loop connector for each line type is connected is shown as a test example.

Execute the `test interfaces` command and the `no test interfaces` command in this order from the operation terminal.

```
> deactivate gigabitethernet 0/1 [Enter]
```

(Connect the loop connector to the corresponding port.)

```
> test interfaces gigabitethernet 0/1 connector [Enter]
```

(Wait about 1 minute.)

```
> no test interfaces gigabitethernet 0/1 [Enter]
```

(Remove the loop connector from the corresponding port and restore the connection.)

```
> activate gigabitethernet 0/1 [Enter]
```

Check the test execution result in the same way for the test execution result of "(1)Checking frame loopback within system."

7

Restarting the System

This chapter describes the procedures for restarting the system.

[7.1 Restarting the System](#)

7.1 Restarting the System

7.1.1 Restarting the System

The system can be restarted by using the `reload` command. Log is stored at restart time. For input format and parameter of the command, see the manual "Operation Commands."

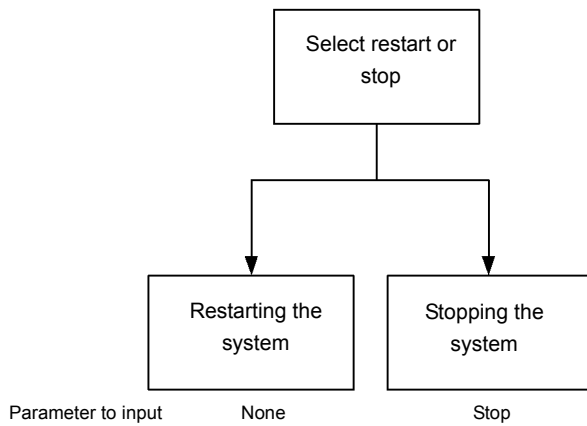
IP8800/S6700, IP8800/S6600, and IP8800/S6300

The following is an example showing how to select the parameter of the `reload` command when "restarting the standby system" and collecting the CPU memory dump of BCU, CSU, and MSU according to the confirmation message.

Step1

Select whether to restart or stop the system.

Figure 7-1: Selecting Restart/Stop of the System

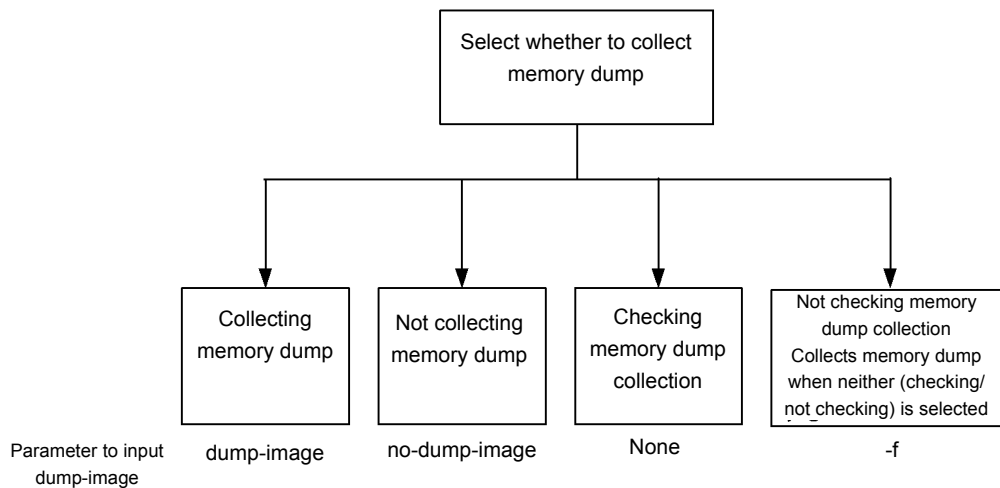


As the standby system is restarted in Step 1, no parameter is selected as shown in figure above.

Step2

Next, select whether to collect the dump.

Figure 7-2: Selecting CPU Memory Dump Type

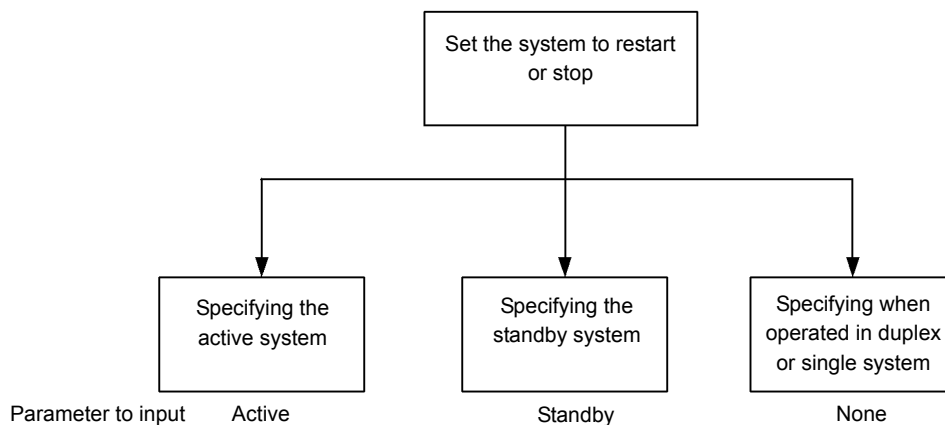


As CPU memory dump is collected in Step 2, no parameter is selected as shown in figure above.

Step3

At last, select which system is restarted or stopped.

Figure 7-3: Selecting the System to Be Restarted or Stopped

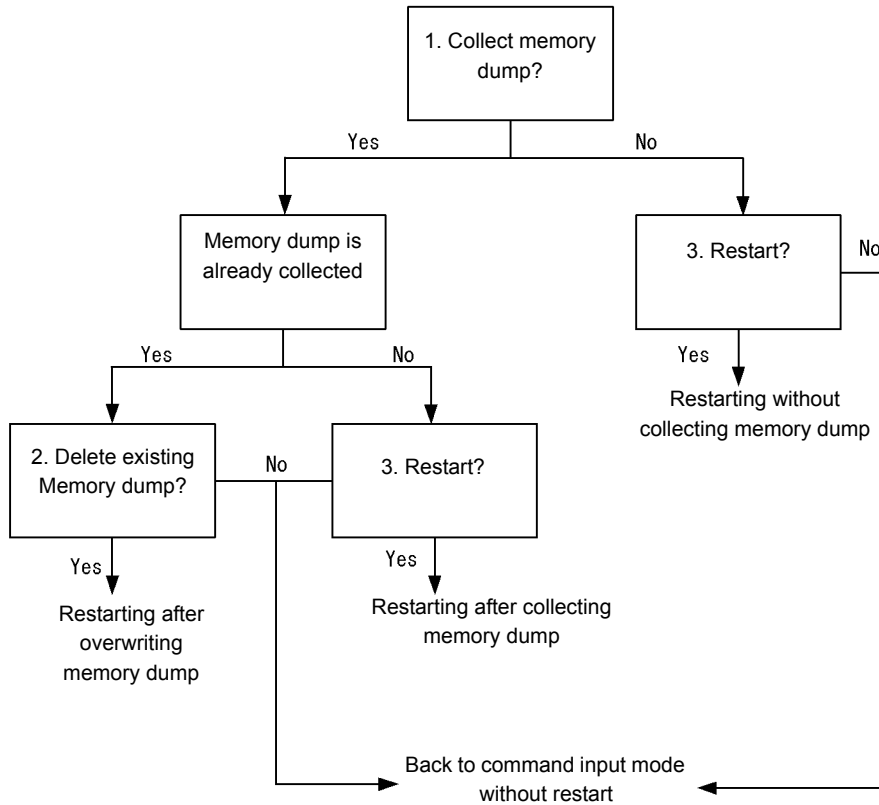


As the standby system is restarted in Step 3, select "standby" as shown in figure above. Combining parameters selected in Step 1 to Step 3 results in "reload standby." Entering this command outputs the dump collection confirmation message as shown below.

1. Dump information extracted?(y/n):_
2. standby :old dump file(rmdump 06/21 18:32) delete OK? (y/n): _
3. Restart OK? (y/n): _

The output timing of above message corresponds to each number in flow chart shown below.

Figure 7-4: Dump Collection Confirmation Message



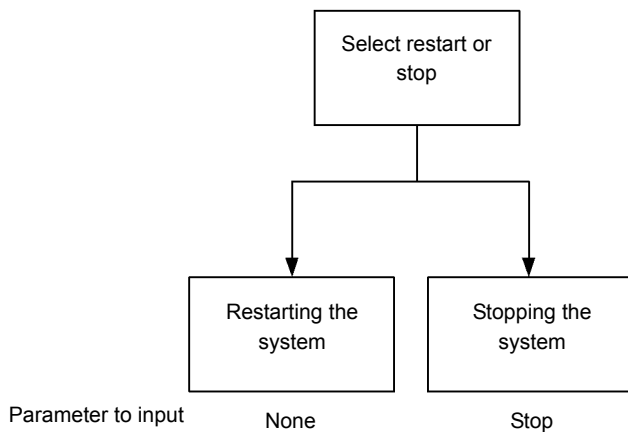
IP8800/S3600 and IP8800/S2400

The following is an example showing how to select the parameter of the `reload` command when restarting the system and collecting the CPU memory dump according to the confirmation message.

Step1

Select whether to restart or stop the system.

Figure 7-5: Selecting Restart/Stop of the System

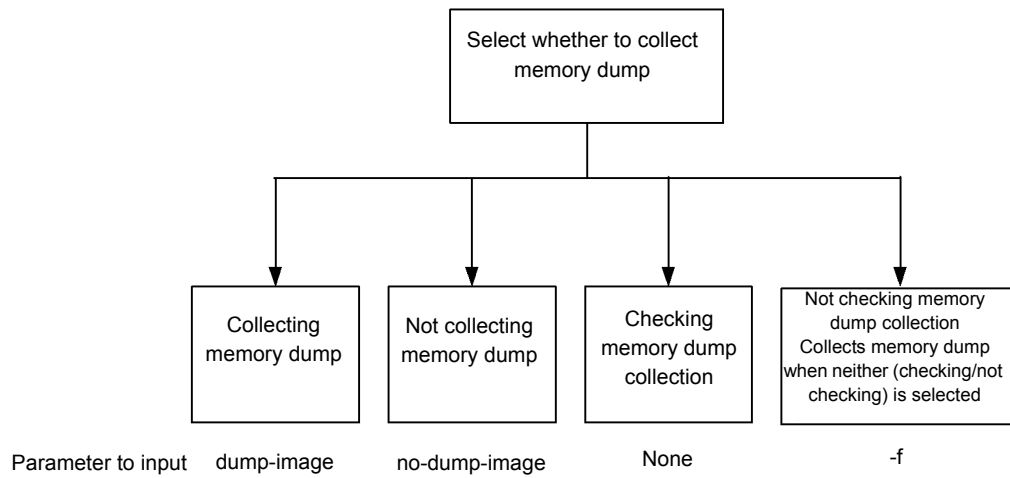


As the system is restarted in Step 1, no parameter is selected as shown in figure above.

Step2

Next, select whether to collect the dump.

Figure 7-6: Selecting CPU Memory Dump Type



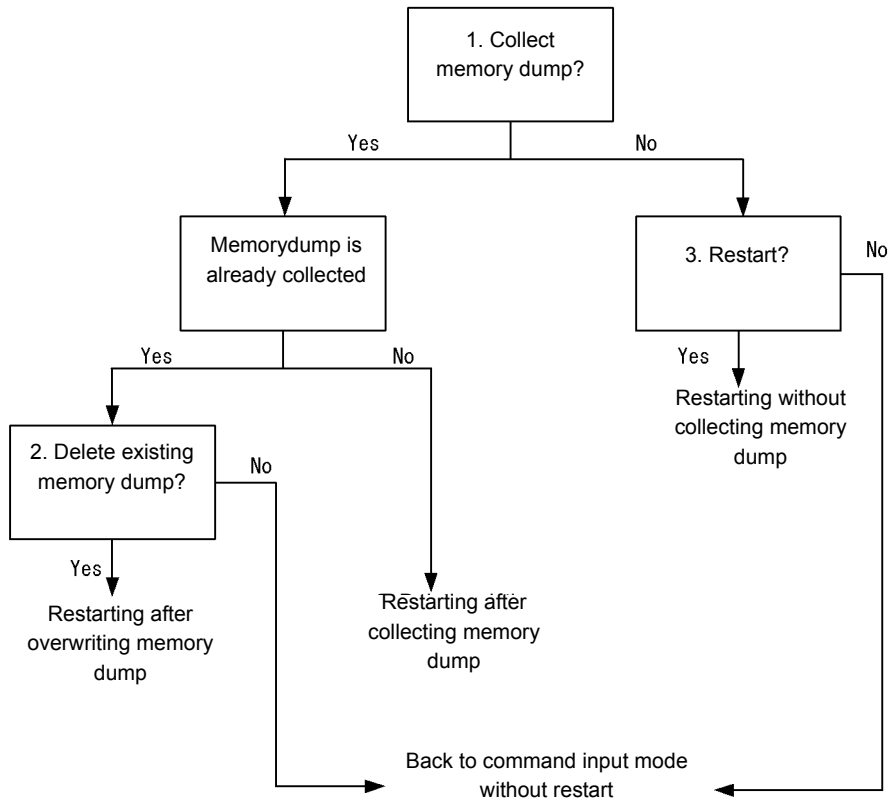
As memory dump is collected in Step 2, no parameter is selected as shown in figure above.

Combining parameters selected in Step 1 and Step 2 results in "reload ." Entering this command outputs the dump collection confirmation message as shown below.

1. Dump information extracted?(y/n):_
2. old dump file(rmdump 01/01 00:00) delete OK? (y/n):_
3. Restart OK? (y/n):_

The output timing of above message corresponds to each number in flow chart shown below.

Figure 7-7: CPU Memory Dump Collection Confirmation Message



Appendix

[Appendix A Contents of show tech-support Command Display](#)

Appendix A Contents of show tech-support Command Display

Appendix A.1 Contents of show tech-support Command Display

The contents of the `show tech-support` command displayed for each protocol parameter are shown in the table below.

For details on the display contents, see "Operation Commands."

[Note]

Some of the information displayed by the show tech-support command is not covered in "Operation Commands." Since such information contains internal information of the system, it is not disclosed to the public.

Besides, please note that some information might not display depending on the software version used.

(1) IP8800/S6700, IP8800/S6600, and IP8800/S6300

The display contents for IP8800/S6700, IP8800/S6600, and IP8800/S6300 are shown in the table below.

Table A-1: Details of Display Contents (IP8800/S6700, IP8800/S6600, IP8800/S6300)

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
1	<code>show version</code>	Software version information and hardware information of this system	Y	Y	Y	Y
2	<code>show license</code>	Optional license information	Y	Y	Y	Y
3	<code>show system</code>	System operating status	Y	Y	Y	Y
4	<code>show environment</code>	FAN/power supply/running time information	Y	Y	Y	Y
5	<code>show process cpu</code>	CPU use information of process	Y	Y	Y	Y
6	<code>show process memory</code>	Memory use information of process	Y	Y	Y	Y
7	<code>show cpu days hours minutes seconds</code>	CPU usage	Y	Y	Y	Y
8	<code>show memory summary</code>	Memory use information of system	Y	Y	Y	Y
9	<code>/sbin/dmesg</code>	Event information in kernel	Y	Y	Y	Y
10	<code>cat /var/run/dmesg.boot</code>	Event information in kernel (for Ver.10.5 and later)	Y	Y	Y	Y
11	<code>cat /var/log/messages</code>	Internal information of kernel and daemon	Y	Y	Y	Y
12	<code>cat /standby/var/run/dmesg.boot</code>	Event information in kernel (for Ver.10.5 and later)	Y	Y	Y	Y
13	<code>cat /standby/var/log/messages</code>	Internal information of kernel and daemon (for Ver.10.5 and later)	Y	Y	Y	Y
14	<code>/usr/local/diag/statShow</code>	Kernel internal statistical information	Y	Y	Y	Y
15	<code>fstat</code>	File descriptor information	Y	Y	Y	Y
16	<code>/usr/local/diag/rtsystat</code>	Internal device related information	Y	Y	Y	Y
17	<code>/usr/local/diag/rtastat</code>	Route distribution related information	Y	Y	Y	Y

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
18	show netstat all-protocol-address numeric	Layer 4 related statistical information	Y	Y	Y	Y
19	show netstat statistics	Layer 3 related statistical information	Y	Y	Y	Y
20	show dumpfile	Sampled dump file information	Y	Y	Y	Y
21	ls -lTiR /dump0	Dump file information	Y	Y	Y	Y
22	ls -lTiR /usr/var/hardware	Hardware dump file information (for Ver.10.5 and later)	Y	Y	Y	Y
23	ls -lTiR /usr/var/core	core file information	Y	Y	Y	Y
24	ls -lTiR /config	config file information	Y	Y	Y	Y
25	ls -lTiR /standby/dump0	Dump file information	Y	Y	Y	Y
26	ls -lTiR /standby/usr/var/ hardware	Hardware dump file information (for Ver.10.5 and later)	Y	Y	Y	Y
27	ls -lTiR /standby/usr/var/ core	core file information	Y	Y	Y	Y
28	ls -lTiR /standby/config	config file information	Y	Y	Y	Y
29	ls -lTiR /var	Memory file system information	Y	Y	Y	Y
30	df -ik	Partition information	Y	Y	Y	Y
31	du -Pk /	File system use status	Y	Y	Y	Y
32	show logging	Active system time series log information	Y	Y	Y	Y
33	show logging reference	Active system type log information	Y	Y	Y	Y
34	show logging standby	Standby system time series log information	Y	Y	Y	Y
35	show logging reference standby	Standby system type log information	Y	Y	Y	Y
36	show ntp associations	ntp server operation information	Y	Y	Y	Y
37	/usr/bin/w -n	Login related information	Y	Y	Y	Y
38	show session	Login session information	Y	Y	Y	Y
39	/usr/sbin/pstat -t	Terminal information	Y	Y	Y	Y
40	stty -a -f /dev/tty00	Console terminal information	Y	Y	Y	Y
41	cat /var/log/clitrace1	CLI trace information 1	Y	Y	Y	Y
42	cat /var/log/clitrace2	CLI trace information 2	Y	Y	Y	Y
43	cat /var/log/mmitrace	Operation command trace information (for Ver.10.5 and later)	Y	Y	Y	Y
44	cat /var/log/kern.log	Kernel internal trace information	Y	Y	Y	Y
45	cat /var/log/daemon.log	Daemon related internal trace information	Y	Y	Y	Y
46	cat /var/log/fixsb.log	Kernel internal trace information (for Ver.10.5 and later)	Y	Y	Y	Y
47	cat /standby/var/log/ kern.log	Kernel internal trace information (for Ver.10.5 and later)	Y	Y	Y	Y
48	cat /standby/var/log/ daemon.log	Daemon related internal trace information (for Ver.10.5 and later)	Y	Y	Y	Y

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
49	cat /standby/var/log/fixsb.log	Kernel internal trace information (for Ver.10.5 and later)	Y	Y	Y	Y
50	cat /usr/var/pplog/ppupdate.log	Log information on updating software (for Ver.11.1 and later)	Y	Y	Y	Y
51	cat /usr/var/pplog/ppupdate2.log	Log information on updating software (for Ver.11.1 and later)	Y	Y	Y	Y
52	cat /standby/usr/var/pplog/ppupdate.log	Log information on updating software (for Ver.11.1 and later)	Y	Y	Y	Y
53	cat /standby/usr/var/pplog/ppupdate2.log	Log information on updating software (for Ver.11.1 and later)	Y	Y	Y	Y
54	tail -n 30 /var/log/authlog	Authentication trace information	Y	Y	Y	Y
55	tail -n 30 /var/log/xferlog	FTP trace information	Y	Y	Y	Y
56	cat /var/log/ssh.log	SSH log information	Y	Y	Y	Y
57	show accounting	Accounting information	Y	Y	Y	Y
58	cat /var/tmp/gen/trace/mng.trc	Configuration command trace information 1	Y	Y	Y	Y
59	tail -n 20 /var/tmp/gen/trace/api.trc	Configuration command trace information 2 (for earlier than Ver.10.7)	Y	Y	Y	Y
60	cat /var/tmp/gen/trace/mng_sub.trc	Configuration command trace information 3 (for Ver.10.7 and later)	Y	Y	Y	Y
61	tail -n 400 /var/tmp/gen/trace/api.trc	Configuration command trace information 4 (for Ver.10.7 and later)	Y	Y	Y	Y
62	tail -n 400 /var/tmp/gen/trace/ctl.trc	Configuration command trace information 5 (for Ver.10.7 and later)	Y	Y	Y	Y
63	show netstat interface	Interface information in kernel	Y	Y	Y	Y
64	show vlan list	VLAN information list	Y	Y	Y	Y
65	show port	Port information	Y	Y	Y	Y
66	show port statistics	Port statistical information	Y	Y	Y	Y
67	show port protocol	Port protocol information	Y	Y	Y	Y
68	show port transceiver debug	Port transceiver detail information	Y	Y	Y	Y
69	show interfaces nif XXX_NIF line XXX_LINE debug	Port detailed statistical information	Y	Y	Y	Y
70	show running-config	Operation configuration	Y	Y	Y	Y
71	show channel-group detail	Link aggregation detail information	Y	Y	Y	Y
72	show spanning-tree detail	Spanning tree detail information	Y	Y	Y	Y
73	show gsrp all	All GSRP detail information	Y	Y	Y	Y
74	show axrp detail	Ring Protocol detail information	Y	Y	Y	Y
75	show efmoam detail	Setting information and port status of IEEE802.3ah/OAM function	Y	Y	Y	Y
76	show efmoam statistics	IEEE802.3ah/OAM function statistical information	Y	Y	Y	Y

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
77	show lldp detail	LLDP function neighboring system information	Y	Y	Y	Y
78	show oadp detail	OADP function neighboring system information	Y	Y	Y	Y
79	show loop-detection	Information on L2 loop detection (for Ver.10.7 and later)	N	N	N	Y
80	show loop-detection statistics	Statistical information on L2 loop detection (for Ver.10.7 and later)	N	N	N	Y
81	show loop-detection logging	Log information on L2 loop detection (for Ver.10.7 and later)	N	N	N	Y
82	show channel-group statistics	Link aggregation statistical information	N	N	N	Y
83	show channel-group statistics lacp	Link aggregation LACP statistical information	N	N	N	Y
84	show spanning-tree statistics	Spanning tree statistical information	N	N	N	Y
85	show vlan detail	VLAN information detail	N	Y	Y	Y
86	show vlan mac-vlan	MAC VLAN information	N	N	N	Y
87	show qos queueing	All queue statistical information	N	Y	Y	Y
		for earlier than Ver.10.6	Y	Y	Y	Y
88	show shaper	Layering shaper statistical information (for Ver.10.7.A and later)	Y	Y	Y	Y
89	show access-filter	Filtering function statistical information	N	Y	Y	Y
90	show qos-flow	QoS control function statistical information	N	Y	Y	Y
91	show lldp statistics	LLDP function statistical information	N	N	N	Y
92	show oadp statistics	OADP function statistical information	N	N	N	Y
93	show mac-address-table	mac-address-table information	N	Y	Y	Y
94	show fense server detail	VAA function FENSE server information	N	N	N	Y
95	show fense statistics	VAA function statistical information	N	N	N	Y
96	show fense logging	VAA function operation log information	N	N	N	Y
97	show dot1x logging	Operation log message sampled for IEEE802.1X authentication	N	N	N	Y
98	show dot1x statistics	Statistical information relating to IEEE802.1X authentication	N	N	N	Y
99	show dot1x detail	Authentication status information relating to IEEE802.X authentication	N	N	N	Y
100	show igmp-snooping	IGMP snooping Information	N	N	N	Y
101	show igmp-snooping group	IGMP snooping group information	N	N	N	Y
102	show igmp-snooping statistics	IGMP snooping statistical information	N	N	N	Y

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
103	show mld-snooping	MLD snooping Information	N	N	N	Y
104	show mld-snooping group	MLD snooping group information	N	N	N	Y
105	show mld-snooping statistics	MLD snooping statistical information	N	N	N	Y
106	show netstat routing-table numeric	Kernel internal route related information (unicast)	N	Y	Y	N
107	show netstat multicast numeric	Kernel internal route related information (multicast)	N	Y	Y	N
108	show ip multicast statistics	IPv4 multicast statistical information (for Ver.10.5 and later, earlier than Ver.11.0) IPv4 multicast statistical information on each VRF (for Ver.11.0 and later)	N	N	Y	N
109	show ipv6 multicast statistics	IPv6 multicast statistical information (for Ver.10.5 and later)	N	N	Y	N
110	show ip igmp interface	Information on interface with IGMP enabled (for earlier than Ver.11.0) Information on interface with VRF-based IGMP enabled (for Ver.11.0 and later)	N	N	Y	N
111	show ip igmp group	Information on group managed by IGMP (for earlier than Ver.11.0) Information on group managed by VRF-based IGMP (for Ver.11.0 and later)	N	N	Y	N
112	show ip pim interface (detail)	Information on Interface with IPv4 PIM enabled (for earlier than Ver.11.0) Information on Interface with VRF-based IPv4 PIM (for Ver.11.0 and later)	N	N	Y	N
113	show ip pim neighbor (detail)	IPv4 PIM neighbor information (for earlier than Ver.11.0) IPv4 PIM neighbor information on each VRF (for Ver.11.0 and later)	N	N	Y	N
114	show ip pim bsr	IPv4 PIM BSR information (for earlier than Ver.11.0) IPv4 PIM BSR information on each VRF (for Ver.11.0 and later)	N	N	Y	N
115	show ip pim rp-mapping	IPv4 PIM rendezvous point information (for earlier than Ver.11.0) IPv4 PIM rendezvous point information on each VRF (for Ver.11.0 and later)	N	N	Y	N
116	show ip mroute	IPv4 multicast routing information (for earlier than Ver.11.0) IPv4 multicast routing information on each VRF (for Ver.11.0 and later)	N	N	Y	N
117	show ip mcache	IPv4 multicast relay entry (for earlier than Ver.11.0) IPv4 multicast relay entry on each VRF (for Ver.11.0 and later)	N	N	Y	N
118	show ipv6 mld interface	Information on interface with MLD enabled	N	N	Y	N

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2	
119	show ipv6 mld group	Information on group managed by MLD	N	N	Y	N	
120	show ipv6 pim interface (detail)	Information on interface with IPv6 PIM enabled	N	N	Y	N	
121	show ipv6 pim neighbor (detail)	IPv6 PIM neighbor information	N	N	Y	N	
122	show ipv6 pim bsr	IPv6 PIM BSR information	N	N	Y	N	
123	show ipv6 pim rp-mapping	IPv6 PIM rendezvous point information	N	N	Y	N	
124	show ipv6 mroute	IPv6 multicast routing information	N	N	Y	N	
125	show ipv6 mcache	IPv6 multicast relay entry	N	N	Y	N	
126	show ip multicast statistics	IPv4 multicast statistical information (for Ver.10.5 and later, earlier than Ver.11.0) IPv4 multicast statistical information on each VRF (for Ver.11.0 and later)	N	N	Y	N	
127	show ipv6 multicast statistics	IPv6 multicast statistical information (for Ver.10.5 and later)	N	N	Y	N	
128	show vrrpstatus detail statistics	VRRP virtual router status and statistical information	N	Y	N	N	
129	show vrrpstatus group	Information on VRRP virtual router grouping (for Ver.11.0 and later)	N	Y	N	N	
130	show vrrpstatus vrrp-vlan	Information on VRRP administrative VLAN (for Ver.11.0 and later)	N	Y	N	N	
131	show track detail	VRRP failure monitoring interface information	N	Y	N	N	
132	show ip interface ipv4-unicast	Interface information of this system recognized by unicast routing program	N	Y	N	N	
133	show processes memory unicast	Memory reservation status and use status in unicast routing program	N	Y	N	N	
134	show processes cpu minutes unicast	CPU usage of unicast routing program	N	Y	N	N	
135	show dhcp giaddr all	DHCP packet destination IP address information of DHCP relay agent	N	Y	N	N	
136	show dhcp traffic	DHCP relay agent statistical information	N	Y	N	N	
137	show ip dhcp server statistics	DHCP server statistical information	N	Y	N	N	
138	show ip dhcp conflict	DHCP Server Conflicted IP address information	N	Y	N	N	
139	show ipv6 dhcp server statistics	IPv6DHCP server statistical information	N	Y	N	N	
140	show ip route summary	Number of active routes and inactive routes reserved by routing protocol	for earlier than Ver.10.6	N	Y	N	N
			for Ver.10.6 and later	Y	Y	Y	Y

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
141	show ip rip statistics	RIP statistical information RIP statistical information on each VRF (for Ver.11.0 and later)	N	Y	N	N
142	show ip rip advertised-routes summary	Number of routes advertised by RIP Number of routes advertised by RIP on each VRF (for Ver.11.0 and later)	N	Y	N	N
143	show ip rip received-routes summary	Number of routes learned by RIP Number of routes learned by RIP on each VRF (for Ver.11.0 and later)	N	Y	N	N
144	show ip ospf	OSPF global information OSPF global information on each VRF (for Ver.11.0 and later)	N	Y	N	N
145	show ip ospf discard-packets	Information on packets discarded by OSPF	N	Y	N	N
146	show ip ospf statistics	Statistical information of sent/ received packets collected by OSPF Statistical information of sent/ received packets collected by OSPF on each VRF (for Ver.11.0 and later)	N	Y	N	N
147	show ip ospf neighbor detail	OSPF neighboring router detail information OSPF neighboring router detail information on each VRF (for Ver.11.0 and later)	N	Y	N	N
148	show ip ospf virtual-links detail	OSPF virtual link detail information OSPF virtual link detail information on each VRF (for Ver.11.0 and later)	N	Y	N	N
149	show ip ospf database database-summary	Number of LSAs for each OSPF LS type Number of LSAs for each OSPF LS type on each VRF (for Ver.11.0 and later)	N	Y	N	N
150	show ip bgp neighbor detail	BGP4 peering information BGP4 peering information on each VRF (for Ver.11.0 and later)	N	Y	N	N
151	show ip bgp notification-factor	Message that caused disconnection of BGP4 connection Message that caused disconnection of BGP4 connection on each VRF (for Ver.11.0 and later)	N	Y	N	N
152	show ip bgp received-routes summary	Number of pieces of routing information received from BGP4 peer Number of pieces of routing information received from BGP4 peer on each VRF (for Ver.11.0 and later)	N	Y	N	N
153	show ip bgp advertised-routes summary	Number of pieces of routing information advertised to BGP4 peer Number of pieces of routing information advertised to BGP4 peer on each VRF (for Ver.11.0 and later)	N	Y	N	N
154	show ip vrf all	Number of routes learned on each VRF (for Ver.11.0 and later)	N	Y	N	N

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2	
155	show graceful-restart unicast	Operation state of the restart router for graceful restart in the unicast routing protocol (for Ver.10.3 and later)	N	Y	N	N	
156	show ipv6 interface ipv6-unicast	Interface information of this system recognized by unicast routing program	N	Y	N	N	
157	show ipv6 route summary	Number of active routes and inactive routes reserved by unicast routing program	for earlier than Ver.10.6	N	Y	N	N
			for Ver.10.6 and later	Y	Y	Y	Y
158	show ipv6 rip advertised-routes summary	Number of routes advertised by RIPng	N	Y	N	N	
159	show ipv6 rip received-routes summary	Number of routes learned by RIPng	N	Y	N	N	
160	show ipv6 rip statistics	RIPng statistical information	N	Y	N	N	
161	show ipv6 ospf	OSPFv3 global information	N	Y	N	N	
162	show ipv6 ospf discard-packets	Information on packets discarded by OSPFv3	N	Y	N	N	
163	show ipv6 ospf statistics	Statistical information of packets collected by OSPFv3	N	Y	N	N	
164	show ipv6 ospf neighbor detail	OSPFv3 neighboring router status	N	Y	N	N	
165	show ipv6 ospf virtual-links detail	OSPFv3 virtual link information	N	Y	N	N	
166	show ipv6 ospf database database-summary	Number of LS-Databases in OSPFv3	N	Y	N	N	
167	show ipv6 bgp neighbor detail	BGP4+ peering information	N	Y	N	N	
168	show ipv6 bgp notification-factor	Packet that caused disconnection of BGP4+ connection	N	Y	N	N	
169	show ipv6 bgp received-routes summary	Number of pieces of routing information received from BGP4+ peer	N	Y	N	N	
170	show ipv6 bgp advertised-routes summary	Number of pieces of routing information advertised to BGP4+ peer	N	Y	N	N	
171	show web-authentication user edit	Display of registrations and changes in built-in WEB authentication DB (for Ver.10.3 and later)	N	N	N	Y	
172	show web-authentication user commit	Display of the registration of built-in Web authentication DB (for Ver.10.3 and later)	N	N	N	Y	
173	show web-authentication statistics	Web authentication statistical information display (for Ver.10.3 and later)	N	N	N	Y	
174	show web-authentication login	Authenticated user information (account information) display (for Ver.10.3 and later)	N	N	N	Y	
175	show web-authentication logging	Web authentication operation log display (for Ver.10.3 and later)	N	N	N	Y	

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
176	show sflow detail	sFlow statistical information (detail) display (for Ver.10.3 and later)	Y	Y	Y	Y
177	show mac-authentication	Display of MAC authentication settings (for Ver.10.6 and later)	N	N	N	Y
178	show mac-authentication statistics	Display of MAC authentication statistical information (for Ver.10.6 and later)	N	N	N	Y
179	show mac-authentication mac-address edit	Display of registrations and changes on the embedded MAC authentication DB (for Ver.10.6 and later)	N	N	N	Y
180	show mac-authentication mac-address commit	Display of the registration of the embedded MAC authentication DB (for Ver.10.6 and later)	N	N	N	Y
181	show mac-authentication login	Display of authenticated user (account) information (for Ver.10.6 and later)	N	N	N	Y
182	show mac-authentication logging	Display of MAC authentication operation logs (for Ver.10.6 and later)	N	N	N	Y
183	show power-control schedule	Display of scheduled power control (for Ver.11.1 and later)	Y	Y	Y	Y
184	pktbusdisp	Display of combination of packet forwarding bus and port number (for Ver.10.7 and later) [IP8800/S6700]	Y	Y	Y	Y
185	nifhdcinfo	NIF HDC information (for Ver.10.7 and later)	Y	Y	Y	Y
186	devstatus	Display of detailed device status (for Ver.11.1 and later)	Y	Y	Y	Y

(Legend) Y: Displayed, N: Hidden

Note: Parenthesis in the column of Command (Display) indicates display depending on the software version.

(2) IP8800/S3600

The display contents for IP8800/S3600 are shown in the table below.

Table A-2: Details of Display Contents (IP8800/S3600)

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
1	show version	Software version information and hardware information of this system	Y	Y	Y	Y
2	show license	Optional license information	Y	Y	Y	Y
3	show system	System operating status	Y	Y	Y	Y
4	show environment	FAN/power supply/running time information	Y	Y	Y	Y
5	show process cpu	CPU use information of process	Y	Y	Y	Y
6	show process memory	Memory use information of process	Y	Y	Y	Y
7	show cpu days hours minutes seconds	CPU usage	Y	Y	Y	Y
8	show memory summary	Memory use information of system	Y	Y	Y	Y

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
9	/sbin/dmesg	Event information in kernel	Y	Y	Y	Y
10	cat /var/run/dmesg.boot	Event information in kernel (for Ver.10.5 and later)	Y	Y	Y	Y
11	cat /var/log/messages	Internal information of kernel and daemon	Y	Y	Y	Y
12	/usr/local/diag/statShow	Kernel internal statistical information	Y	Y	Y	Y
13	fstat	File descriptor information	Y	Y	Y	Y
14	/usr/local/diag/rtsystat	Internal device related information	Y	Y	Y	Y
15	/usr/local/diag/rtastat	Route distribution related information	Y	Y	Y	Y
16	show netstat all-protocol-address numeric	Layer 4 related statistical information	Y	Y	Y	Y
17	show netstat statistics	Layer 3 related statistical information	Y	Y	Y	Y
18	show dumpfile	Sampled dump file information	Y	Y	Y	Y
19	ls -lTiR /dump0	Dump file information	Y	Y	Y	Y
20	ls -lTiR /usr/var/hardware	Hardware dump file information (Ver.10.5 and later)	Y	Y	Y	Y
21	ls -lTiR /usr/var/core	core file information	Y	Y	Y	Y
22	ls -lTiR /config	config file information	Y	Y	Y	Y
23	ls -lTiR /var	Memory file system information (Ver.10.1.A and later)	Y	Y	Y	Y
24	df -ik	Partition information	Y	Y	Y	Y
25	du -Pk /	File system use status	Y	Y	Y	Y
26	show logging	Operational time-series log information	Y	Y	Y	Y
27	show logging reference	Operational type-basis log information	Y	Y	Y	Y
28	show ntp associations	NTP server operation information	Y	Y	Y	Y
29	/usr/bin/w -n	Login related information	Y	Y	Y	Y
30	last -30	Login history (10.1.A and earlier)	Y	Y	Y	Y
31	show session	Login session information	Y	Y	Y	Y
32	/usr/sbin/pstat -t	Terminal information	Y	Y	Y	Y
33	stty -a -f /dev/tty00	Console terminal information	Y	Y	Y	Y
34	ls -lTiR /var/tmp/mmi*	CLI information file list (10.1.A and earlier)	Y	Y	Y	Y
35	cat /var/log/clitrace1	CLI trace information 1	Y	Y	Y	Y
36	cat /var/log/clitrace2	CLI trace information 2	Y	Y	Y	Y
37	cat /var/log/mmitrace	Operation command trace information (Ver.10.5 and later)	Y	Y	Y	Y
38	cat /var/log/kern.log	Kernel internal trace information	Y	Y	Y	Y
39	cat /var/log/daemon.log	Daemon related internal trace information	Y	Y	Y	Y
40	cat /var/log/fixsb.log	Kernel internal trace information (Ver.10.5 and later)	Y	Y	Y	Y

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
41	cat /usr/var/pplog/ppupdate.log	Log information during software update (for Ver.11.1 and later)	Y	Y	Y	Y
42	cat /usr/var/pplog/ppupdate2.log	Log information during software update (for Ver.11.1 and later)	Y	Y	Y	Y
43	tail -n 30 /var/log/authlog	Authentication trace information	Y	Y	Y	Y
44	tail -n 30 /var/log/xferlog	FTP trace information	Y	Y	Y	Y
45	cat /var/log/ssh.log	SSH log information	Y	Y	Y	Y
46	show accounting	Accounting information	Y	Y	Y	Y
47	cat /var/tmp/gen/trace/mng.trc	Configuration command trace information 1	Y	Y	Y	Y
48	tail -n 20 /var/tmp/gen/trace/api.trc	Configuration command trace information 2 (for Ver.10.7 and earlier)	Y	Y	Y	Y
49	cat /var/tmp/gen/trace/mng_sub.trc	Configuration command trace information 3 (for Ver.10.7 and later)	Y	Y	Y	Y
50	tail -n 400 /var/tmp/gen/trace/api.trc	Configuration command trace information 4 (for Ver.10.7 and later)	Y	Y	Y	Y
51	tail -n 400 /var/tmp/gen/trace/ctl.trc	Configuration command trace information 5 (for Ver.10.7 and later)	Y	Y	Y	Y
52	show netstat interface	Interface information in kernel	Y	Y	Y	Y
53	show vlan list	VLAN information list	Y	Y	Y	Y
54	show port	Port information	Y	Y	Y	Y
55	show port statistics	Port statistical information	Y	Y	Y	Y
56	show port protocol	Port protocol information	Y	Y	Y	Y
57	show port transceiver debug	Port transceiver detail information	Y	Y	Y	Y
58	show interfaces nif XXX_NIF line XXX_LINE debug	Port detailed statistical information	Y	Y	Y	Y
59	show power inline	PoE information	Y	Y	Y	Y
60	show running-config	Operation configuration	Y	Y	Y	Y
61	show channel-group detail	Link aggregation detail information	Y	Y	Y	Y
62	show spanning-tree detail	Spanning tree detail information	Y	Y	Y	Y
63	show gsrp all	All GSRP detail information	Y	Y	Y	Y
64	show axrp detail	Ring Protocol detail information	Y	Y	Y	Y
65	show efmoam detail	Setting information and port status of IEEE802.3ah/OAM function	Y	Y	Y	Y
66	show efmoam statistics	IEEE802.3ah/OAM function statistical information	Y	Y	Y	Y
67	show lldp detail	LLDP function neighboring system information	Y	Y	Y	Y
68	show oadp detail	OADP function neighboring system information	Y	Y	Y	Y

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2	
69	show loop-detection	Information on L2 Loop detection function (for Ver.10.7 and later)	N	N	N	Y	
70	show loop-detection statistics	Statistics information on L2 Loop detection function (for Ver.10.7 and later)	N	N	N	Y	
71	sshow loop-detection logging	Log information on L2 Loop detection function (for Ver.10.7 and later)	N	N	N	Y	
72	show channel-group statistics	Link aggregation statistical information	N	N	N	Y	
73	show channel-group statistics lacp	Link aggregation LACP statistical information	N	N	N	Y	
74	show spanning-tree statistics	Spanning tree statistical information	N	N	N	Y	
75	show vlan detail	VLAN information detail	N	Y	Y	Y	
76	show vlan mac-vlan	MAC VLAN information	N	N	N	Y	
77	show qos queueing	All queue statistical information	Ver.10.6 and earlier	N	Y	Y	Y
			Ver.10.6 and later	Y	Y	Y	Y
78	show access-filter	Filtering function statistical information	N	Y	Y	Y	
79	show qos-flow	QoS control function statistical information	N	Y	Y	Y	
80	show lldp statistics	LLDP function statistical information	N	N	N	Y	
81	show oadp statistics	OADP function statistical information	N	N	N	Y	
82	show mac-address-table	mac-address-table information	N	Y	Y	Y	
83	show fense server detail	VAA function FENSE server information	N	N	N	Y	
84	show fense statistics	VAA function statistical information	N	N	N	Y	
85	show fense logging	VAA function operation log information	N	N	N	Y	
86	show dot1x logging	Operation log message sampled for IEEE802.1X authentication	N	N	N	Y	
87	show dot1x statistics	Statistical information relating to IEEE802.1X authentication	N	N	N	Y	
88	show dot1x detail	Authentication status information relating to IEEE802.X authentication	N	N	N	Y	
89	show igmp-snooping	IGMP snooping Information	N	N	N	Y	
90	show igmp-snooping group	IGMP snooping group information	N	N	N	Y	
91	show igmp-snooping statistics	IGMP snooping statistical information	N	N	N	Y	
92	show mld-snooping	MLD snooping Information	N	N	N	Y	
93	show mld-snooping group	MLD snooping group information	N	N	N	Y	
94	show mld-snooping statistics	MLD snooping statistical information	N	N	N	Y	
95	show netstat routing-table numeric	Kernel internal route related information (unicast)	N	Y	Y	N	

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
96	show netstat multicast numeric	Kernel internal route related information (multicast)	N	N	Y	N
97	show ip multicast statistics	Statistics information on IPv4 multicast (for Ver.10.5 and later)	N	N	Y	N
98	show ipv6 multicast statistics	Statistics information on IPv6 multicast (for Ver.10.5 and later)	N	N	Y	N
99	show ip igmp interface	Interface information for running IGMP	N	N	Y	N
100	show ip igmp group	Group information managed by IGMP	N	N	Y	N
101	show ip pim interface	Interface information for running IPv4 PIM	N	N	Y	N
102	show ip pim neighbor	IPv4 PIM adjacency information	N	N	Y	N
103	show ip pim bsr	IPv4 PIM BSR information	N	N	Y	N
104	show ip pim rp-mapping	IPv4 PIM rendezvous point information	N	N	Y	N
105	show ip mroute	IPv4 multicast route information	N	N	Y	N
106	show ip mcache	IPv4 multicast relay entry	N	N	Y	N
107	show ipv6 mld interface	Interface information for running MLD	N	N	Y	N
108	show ipv6 mld group	Group information managed by MLD	N	N	Y	N
109	show ipv6 pim interface	Interface information for running IPv6 PIM	N	N	Y	N
110	show ipv6 pim neighbor	IPv6 PIM adjacency information	N	N	Y	N
111	show ipv6 pim bsr	IPv6 PIM BSR information	N	N	Y	N
112	show ipv6 pim rp-mapping	IPv6 PIM rendezvous point information	N	N	Y	N
113	show ipv6 mroute	IPv6 multicast route information	N	N	Y	N
114	show ipv6 mcache	IPv6 multicast relay entry	N	N	Y	N
115	show ip multicast statistics	IPv4 multicast statistical information (for Ver.10.5 and later)	N	N	Y	N
116	show ipv6 multicast statistics	IPv6 multicast statistical information (for Ver.10.5 and later)	N	N	Y	N
117	show vrrpstatus detail statistics	VRRP virtual router status and statistical information	N	Y	N	N
118	show track detail	VRRP failure monitoring interface information	N	Y	N	N
119	show ip interface ipv4-unicast	Interface information of this system recognized by unicast routing program	N	Y	N	N
120	show processes memory unicast	Memory reservation status and use status in unicast routing program	N	Y	N	N
121	show processes cpu minutes unicast	CPU usage of unicast routing program	N	Y	N	N
122	show dhcp giaddr all	DHCP packet destination IP address information of DHCP relay agent	N	Y	N	N
123	show dhcp traffic	DHCP relay agent statistical information	N	Y	N	N

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2	
124	show ip dhcp server statistics	DHCP server statistical information	N	Y	N	N	
125	show ip dhcp conflict	DHCP Server Conflicted IP address information	N	Y	N	N	
126	show ipv6 dhcp server statistics	IPv6DHCP server statistical information	N	Y	N	N	
127	show ip route summary	Number of active routes and inactive routes reserved by routing protocol	Ver.10.6 and earlier	N	Y	N	N
			Ver.10.6 and later	Y	Y	Y	Y
128	show ip rip statistics	RIP statistical information	N	Y	N	N	
129	show ip rip advertised-routes summary	Number of routes advertised by RIP	N	Y	N	N	
130	show ip rip received-routes summary	Number of routes learned by RIP	N	Y	N	N	
131	show ip ospf	OSPF global information	N	Y	N	N	
132	show ip ospf discard-packets	Packet information discarded by OSPF	N	Y	N	N	
133	show ip ospf statistics	Statistical information of sent/received packets collected by OSPF	N	Y	N	N	
134	show ip ospf neighbor detail	OSPF neighboring router detail information	N	Y	N	N	
135	show ip ospf virtual-links detail	OSPF virtual link detail information	N	Y	N	N	
136	show ip ospf database database-summary	Number of LSAs by OSPF LS type	N	Y	N	N	
137	show ip bgp neighbor detail	BGP4 peering information	N	Y	N	N	
138	show ip bgp notification-factor	Message that caused disconnection of BGP4 connection	N	Y	N	N	
139	show ip bgp received-routes summary	Number of route information received from BGP4 peer	N	Y	N	N	
140	show ip bgp advertised-routes summary	Number of route information advertised to BGP4 peer	N	Y	N	N	
141	show ipv6 interface ipv6-unicast	Interface information of this system recognized by unicast routing program	N	Y	N	N	
142	show ipv6 route summary	Number of active routes and inactive routes reserved by unicast routing program	Ver.10.6 and earlier	N	Y	N	N
			Ver.10.6 and later	Y	Y	Y	Y
143	show ipv6 rip advertised-routes summary	Number of routes advertised by RIPng	N	Y	N	N	
144	show ipv6 rip received-routes summary	Number of routes learned by RIPng	N	Y	N	N	
145	show ipv6 rip statistics	RIPng statistical information	N	Y	N	N	
146	show ipv6 ospf	OSPFv3 global information	N	Y	N	N	

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
147	show ipv6 ospf discard-packets	Packet information discarded by OSPFv3	N	Y	N	N
148	show ipv6 ospf statistics	Statistical information of packets collected by OSPFv3	N	Y	N	N
149	show ipv6 ospf neighbor detail	OSPFv3 neighboring router status	N	Y	N	N
150	show ipv6 ospf virtual-links detail	OSPFv3 virtual link information	N	Y	N	N
151	show ipv6 ospf database database-summary	Number of LS-Databases in OSPFv3	N	Y	N	N
152	show ipv6 bgp neighbor detail	BGP4+ peering information	N	Y	N	N
153	show ipv6 bgp notification-factor	Packet that caused disconnection of BGP4+ connection	N	Y	N	N
154	show ipv6 bgp received-routes summary	Number of route information received from BGP4+ peer	N	Y	N	N
155	show ipv6 bgp advertised-routes summary	Number of route information advertised to BGP4+ peer	N	Y	N	N
156	show web-authentication user edit	Display of registration/change contents in built-in WEB authentication DB (for Ver.10.3 and later)	N	N	N	Y
157	show web-authentication user commit	Display of registration contents in built-in Web authentication DB (for Ver.10.3 and later)	N	N	N	Y
158	show web-authentication statistics	Web authentication statistical information display (for Ver.10.3 and later)	N	N	N	Y
159	show web-authentication login	Authenticated user information (account information) display (for Ver.10.3 and later)	N	N	N	Y
160	show web-authentication logging	Web authentication operation log display (Ver.10.3 and later)	N	N	N	Y
161	show sflow detail	sFlow statistical information (detail) display (for Ver.10.4 and later)	Y	Y	Y	Y
162	port snd/rcv statistics	Port sending/receiving statistical information	Y	Y	Y	Y
163	internal SW HW event statistics0	Internal SW event statistics information 0 (for Ver.10.5 and later)	Y	Y	Y	Y
164	internal SW HW event statistics1	Internal SW event statistics information 0 (for Ver.10.5 and later)	Y	Y	Y	Y
165	show mac-authentication	MAC authentication setting information 0 (for Ver.10.6 and later)	N	N	N	Y
166	show mac-authentication statistics	MAC authentication statistics information 0 (for Ver.10.6 and later)	N	N	N	Y
167	show mac-authentication mac-address edit	Display of internal MAC authentication DB registration/change (for Ver.10.6 and later)	N	N	N	Y

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
168	show mac-authentication mac-address commit	Display of internal MAC authentication DB registration (Ver.10.6 and later)	N	N	N	Y
169	show mac-authentication login	Authenticated user information (account information) display (for Ver.10.6 and later)	N	N	N	Y
170	show mac-authentication logging	MAC authentication activity log display (for Ver.10.6 and later)	N	N	N	Y
171	swdev logging	Display of SW logs (for Ver.11.1.C and later)	Y	Y	Y	Y

(Legend) Y: Displayed, N: Hidden

Note: Parenthesis in the column of Command (Display) indicates display depending on the software version.

(3) IP8800/S2400

The display contents for IP8800/S2400 are shown in the table below.

Table A-3: Details of Display Contents (IP8800/S2400)

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
1	show version	Software version information and hardware information of this system	Y	Y	Y	Y
2	show license	Optional license information	Y	Y	Y	Y
3	show system	System operating status	Y	Y	Y	Y
4	show environment	FAN/power supply/running time information	Y	Y	Y	Y
5	show process cpu	CPU use information of process	Y	Y	Y	Y
6	show process memory	Memory use information of process	Y	Y	Y	Y
7	show cpu days hours minutes seconds	CPU usage	Y	Y	Y	Y
8	show memory summary	Memory use information of system	Y	Y	Y	Y
9	/sbin/dmesg	Event information in kernel	Y	Y	Y	Y
10	cat /var/run/dmesg.boot	Event information in kernel (for Ver.10.5 and later)	Y	Y	Y	Y
11	cat /var/log/messages	Internal information of kernel and daemon	Y	Y	Y	Y
12	/usr/local/diag/statShow	Kernel internal statistical information	Y	Y	Y	Y
13	fstat	File descriptor information	Y	Y	Y	Y
14	/usr/local/diag/rtsystat	Internal device related information	Y	Y	Y	Y
15	/usr/local/diag/rtastat	Route distribution related information	Y	Y	Y	Y
16	show netstat all-protocol-address numeric	Layer 4 related statistical information	Y	Y	Y	Y
17	show netstat statistics	Layer 3 related statistical information	Y	Y	Y	Y
18	show dumpfile	Sampled dump file information	Y	Y	Y	Y

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
19	ls -lTiR /dump0	Dump file information	Y	Y	Y	Y
20	ls -lTiR /usr/var/hardware	Hardware dump file information (for Ver.10.5 and later)	Y	Y	Y	Y
21	ls -lTiR /usr/var/core	core file information	Y	Y	Y	Y
22	ls -lTiR /config	config file information	Y	Y	Y	Y
23	ls -lTiR /var	Memory file system information (for Ver.10.1.A and later)	Y	Y	Y	Y
24	df -ik	Partition information	Y	Y	Y	Y
25	du -Pk /	File system use status	Y	Y	Y	Y
26	show logging	Operational time series log information	Y	Y	Y	Y
27	show logging reference	Operational type-basis log information	Y	Y	Y	Y
28	show ntp associations	NTP server operation information	Y	Y	Y	Y
29	/usr/bin/w -n	Login related information	Y	Y	Y	Y
30	last -30	Login history (for earlier than Ver.10.1.A)	Y	Y	Y	Y
31	show session	Login session information	Y	Y	Y	Y
32	/usr/sbin/pstat -t	Terminal information	Y	Y	Y	Y
33	stty -a -f /dev/tty00	Console terminal information	Y	Y	Y	Y
34	ls -lTiR /var/tmp/mmi*	List of CLI-information files (for earlier than Ver.10.1.A)	Y	Y	Y	Y
35	cat /var/log/clitrace1	CLI trace information 1	Y	Y	Y	Y
36	cat /var/log/clitrace2	CLI trace information 2	Y	Y	Y	Y
37	cat /var/log/mmimtrace	Operation command trace information (for Ver.10.5 and later)	Y	Y	Y	Y
38	cat /var/log/kern.log	Kernel internal trace information	Y	Y	Y	Y
39	cat /var/log/daemon.log	Daemon related internal trace information	Y	Y	Y	Y
40	cat /var/log/fixsb.log	Kernel internal trace information (for Ver.10.5 and later)	Y	Y	Y	Y
41	cat /usr/var/pplog/ppupdate.log	Log information on updating software (for Ver.11.1 and later)	Y	Y	Y	Y
42	cat /usr/var/pplog/ppupdate2.log	Log information on updating software (for Ver.11.1 and later)	Y	Y	Y	Y
43	tail -n 30 /var/log/authlog	Authentication trace information	Y	Y	Y	Y
44	tail -n 30 /var/log/xferlog	FTP trace information	Y	Y	Y	Y
45	cat /var/log/ssh.log	SSH log information	Y	Y	Y	Y
46	show accounting	Accounting information	Y	Y	Y	Y
47	cat /var/tmp/gen/trace/mng.trc	Configuration command trace information 1	Y	Y	Y	Y
48	tail -n 20 /var/tmp/gen/trace/api.trc	Configuration command trace information 2 (for earlier than Ver.10.7)	Y	Y	Y	Y

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
49	cat /var/tmp/gen/trace/mng_sub.trc	Configuration command trace information 3 (for Ver.10.7 and later)	Y	Y	Y	Y
50	tail -n 400 /var/tmp/gen/trace/api.trc	Configuration command trace information 4 (for Ver.10.7 and later)	Y	Y	Y	Y
51	tail -n 400 /var/tmp/gen/trace/ctl.trc	Configuration command trace information 5 (for Ver.10.7 and later)	Y	Y	Y	Y
52	show netstat interface	Interface information in kernel	Y	Y	Y	Y
53	show vlan list	VLAN information list	Y	Y	Y	Y
54	show port	Port information	Y	Y	Y	Y
55	show port statistics	Port statistical information	Y	Y	Y	Y
56	show port protocol	Port protocol information	Y	Y	Y	Y
57	show port transceiver debug	Port transceiver detail information	Y	Y	Y	Y
58	show interfaces nif XXX_NIF line XXX_LINE debug	Port detailed statistical information	Y	Y	Y	Y
59	show running-config	Operation configuration	Y	Y	Y	Y
60	show channel-group detail	Link aggregation detail information	Y	Y	Y	Y
61	show spanning-tree detail	Spanning tree detail information	Y	Y	Y	Y
62	show gsrp all	All GSRP detail information	Y	Y	Y	Y
63	show axrp detail	Ring Protocol detail information	Y	Y	Y	Y
64	show efmoam detail	Setting information and port status of IEEE802.3ah/OAM function	Y	Y	Y	Y
65	show efmoam statistics	IEEE802.3ah/OAM function statistical information	Y	Y	Y	Y
66	show lldp detail	LLDP function neighboring system information	Y	Y	Y	Y
67	show oadp detail	OADP function neighboring system information	Y	Y	Y	Y
68	show loop-detection	Information on L2 loop detection (for Ver.10.7 and later)	N	N	N	Y
69	show loop-detection statistics	Statistical information on L2 loop detection (for Ver.10.7 and later)	N	N	N	Y
70	show loop-detection logging	Log information on L2 loop detection (for Ver.10.7 and later)	N	N	N	Y
71	show channel-group statistics	Link aggregation statistical information	N	N	N	Y
72	show channel-group statistics lacp	Link aggregation LACP statistical information	N	N	N	Y
73	show spanning-tree statistics	Spanning tree statistical information	N	N	N	Y
74	show vlan detail	VLAN information detail	N	Y	Y	Y
75	show vlan mac-vlan	MAC VLAN information	N	N	N	Y

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2	
76	show qos queueing	All queue statistical information	for earlier than Ver.10.6	N	Y	Y	Y
			for Ver.10.6 and later	Y	Y	Y	Y
77	show access-filter	Filtering function statistical information	N	Y	Y	Y	
78	show qos-flow	QoS control function statistical information	N	Y	Y	Y	
79	show lldp statistics	LLDP function statistical information	N	N	N	Y	
80	show oadp statistics	OADP function statistical information	N	N	N	Y	
81	show mac-address-table	mac-address-table information	N	Y	Y	Y	
82	show fense server detail	VAA function FENSE server information	N	N	N	Y	
83	show fense statistics	VAA function statistical information	N	N	N	Y	
84	show fense logging	VAA function operation log information	N	N	N	Y	
85	show dot1x logging	Operation log message sampled for IEEE802.1X authentication	N	N	N	Y	
86	show dot1x statistics	Statistical information relating to IEEE802.1X authentication	N	N	N	Y	
87	show dot1x detail	Authentication status information relating to IEEE802.X authentication	N	N	N	Y	
88	show igmp-snooping	IGMP snooping Information	N	N	N	Y	
89	show igmp-snooping group	IGMP snooping group information	N	N	N	Y	
90	show igmp-snooping statistics	IGMP snooping statistical information	N	N	N	Y	
91	show mld-snooping	MLD snooping Information	N	N	N	Y	
92	show mld-snooping group	MLD snooping group information	N	N	N	Y	
93	show mld-snooping statistics	MLD snooping statistical information	N	N	N	Y	
94	show web-authentication user edit	Display of registrations and changes on the built-in WEB authentication DB (for Ver.10.3 and later)	N	N	N	Y	
95	show web-authentication user commit	Display of the registration of the built-in Web authentication DB (for Ver.10.3 and later)	N	N	N	Y	
96	show web-authentication statistics	Web authentication statistical information display (for Ver.10.3 and later)	N	N	N	Y	
97	show web-authentication login	Authenticated user (account) information display (for Ver.10.3 and later)	N	N	N	Y	
98	show web-authentication logging	Web authentication operation log display (for Ver.10.3 and later)	N	N	N	Y	
99	show sflow detail	sFlow statistical information (detail) display (for Ver.10.4 and later)	Y	Y	Y	Y	

No.	Command (Display)	Description	No Parameter Specified	unicast	multi cast	layer-2
100	port snd/rcv statistics	Port sending/receiving statistical information	Y	Y	Y	Y
101	internal SW HW event statistics0	Internal SW event statistical information 0 (for Ver.10.5 and later)	Y	Y	Y	Y
102	internal SW HW event statistics1	Internal SW event statistical information 1 (for Ver.10.5 and later)	Y	Y	Y	Y
103	show mac-authentication	Display of MAC authentication settings (for Ver.10.6 and later)	N	N	N	Y
104	show mac-authentication statistics	Display of MAC authentication statistical information (for Ver.10.6 and later)	N	N	N	Y
105	show mac-authentication mac-address edit	Display of registrations and changes on the embedded MAC authentication DB (for Ver.10.6 and later)	N	N	N	Y
106	show mac-authentication mac-address commit	Display of the registration of embedded MAC authentication DB (for Ver.10.6 and later)	N	N	N	Y
107	show mac-authentication login	Display of authenticated user (account) information (for Ver.10.6 and later)	N	N	N	Y
108	show mac-authentication logging	Display of MAC authentication operation logs (for Ver.10.6 and later)	N	N	N	Y
109	swdev logging	Display of SW logs (Ver.11.1.C and later)	Y	Y	Y	Y

(Legend) Y: Displayed, N: Hidden

Note: Parenthesis in the column of Command (Display) indicates display depending on the software version.

Index

Symbols

"MC not found" is displayed when MC is accessed 22

"MC:-----" is displayed by entering the show system command or the show mc command 22

A

Action to Be Taken When MAC Address Table Resource Shortage Occurs 130

Action to Be Taken When Resource Shortage of Shared Memory Occurs 135

Action to Be Taken When VLAN Identification Table Resource Shortage Occurs 133

Actions against Troubles on 1000BASE-X 32

Actions against Troubles on 10BASE-T/100BASE-TX/1000BASE-T 30

Actions against Troubles on 10GBASE-R 33

Active BSU Switchover Is Disabled 121

Active System Switchover Is Disabled 120

C

Checking Filtering/QoS Setting Information 126

Checking Resource Usage of MAC Address Table 130

Checking Resource Usage of Shared Memory 135

Checking VLAN Identification Table Resource Usage 133

Collecting Failure Information 137, 138

Collecting Failure Information Using dump Command 140

Collecting Failure Information Using ftp Command from the Operation Terminal 138

Command Authorization Using RADIUS/TACACS+ Is Disabled 25

Communication Failure Caused by Settings of Filtering/QoS 126

Communication Failure in Basic Switching Unit BSU/PSP 29

Communication Failure on High-reliability Function 103

Communication Failure on IEEE802.3ah/UDLD Function 119

Communication Failure on Using Authentication VLAN 99

Communication Failure on Using IEEE 802.1X 89

Communication Failure on Using Link Aggregation 36

Communication Failure on Using MAC Authentication 97

Communication Failure on Using PoE 35

Communication Failure on Using Web Authentication 92

Communication Failures on Neighboring System Managing Function 116

Communication Is Disabled or Is Disconnected [IPv4] 50

Communication Is Disabled or Is Disconnected [IPv6] 71

Communication on IPv4 PIM-SM Network Is Disabled 63

Communication on IPv4 PIM-SSM Network Is Disabled 67

Communication on IPv6 PIM-SM Network Is Disabled 81

Communication on IPv6 PIM-SSM Network Is Disabled 85

Communication with VRRP Configuration in IPv4 Network Is Disabled 105

Communication with VRRP Configuration in IPv6 Network Is Disabled 107

Congestion Caused by Packets Processed Through CPU Is Not Recovered 124

Contents of show tech-support Command Display 166

Counter Sample Does Not Reach Collector 115

E

Ethernet Port 154

Ethernet Port Cannot Be Connected 27

F

Failure Analysis for IP8800/S3600 and IP8800/S2400 4

Failure Analysis for IP8800/S6700 and IP8800/S6300 3

Failure Analysis Overview 2

Failures on Using Ring Protocol 41

Failures on Using Spanning Tree 40

Flow Sample Does Not Reach Collector 115

Forgot the Login User Password 21

Forgot the System Administrator Password 21

Functional Failure Analysis Overview 7

G

GSRP Communication Failures 103

I

IP Addresses Cannot Be Assigned Using DHCP Function 54

IPv4 Multicast Communication Failure In VRF 70

IPv4 Multicast Routing Communication Failure 63

IPv4 Network Communication Failure 50

IPv4 Unicast Routing Communication Failure 61

IPv6 DHCP Troubleshooting 73

IPv6 Multicast Routing Communication Failure 81

IPv6 Network Communication Failure 71

IPv6 Unicast Routing Communication Failure 79

Isolating Failures on External Power Unit 17

L

- Layer 2 Authentication Communication Failure 89
- Layer 2 Communication by VLAN Is Disabled 38
- Layer 2 Network Communication Failure 38
- Login Authentication Using RADIUS/TACACS+ Is Disabled 25
- Login from the Remote Operation Terminal Is Disabled 24

M

- MAC Address Table Resource Shortage 130
- MIBs Cannot Be Obtained from SNMP Manager 110
- Multicast Data Is Double-relayed on IPv4 PIM-SM Network 66
- Multicast Data Is Double-relayed on IPv4 PIM-SSM Network 69
- Multicast Data Is Double-relayed on IPv6 PIM-SM Network 84
- Multicast Data Is Double-relayed on IPv6 PIM-SSM Network 87
- Multicast Relay by IGMP snooping Is Disabled 44
- Multicast Relay by MLD snooping Is Disabled 47

N

- Network Interface Communication Failure 27
- No BGP4 Routing Information Exists 62
- No BGP4+ Routing Information Exists 80
- No OSPF Routing Information Exists 61
- No OSPFv3 Routing Information Exists 79
- No RIP Routing Information Exists 61
- No RIPng Routing Information Exists 79
- No Routing Information Exist 62
- NTP Communication Failure 118

O

- Overview 1

P

- Port Becomes Inactive Due to IEEE802.3ah/UDLD Function 119
- Problems on Login Password 21
- Problems on MC 22
- Problems on Operation Terminal 23
- Problems on Power Saving Feature 123
- Problems on Redundant Configuration of Basic Control Unit (BCU)/Control and Switching Unit (CSU)/Management and Switching Unit (MSU) 120

- Problems on Redundant Configuration of Basic Switching Unit (BSU) 121

R

- Restarting the System 160

S

- Schedule Is Disabled 123
- sFlow Packets Does not Reach Collector 112
- SNMP Communication Failure 110
- System and Partial Failure Analysis Overview 3

T

- Testing Line 154
- Time Synchronization by NTP Is Disabled 118
- Transferring Files for Maintenance Information 144
- Transferring Files Using ftp Command 145
- Transferring Files Using ftp Command from the Operation Terminal 150
- Transferring Files Using zmodem Command 148
- Transferring Maintenance Information Files Using show tech-support Command 148
- Traps Cannot Be Received by SNMP Manager 110
- Troubleshooting for IP8800/S3600 and IP8800/S2400 15
- Troubleshooting for IP8800/S6700 and IP8800/S6300 12
- Troubleshooting of sFlow Statistics (Flow Statistics) Function 112
- Troubleshooting Procedure on System Failures [IP8800/S3600 and IP8800/S2400] 15
- Troubleshooting Procedure on System Failures [IP8800/S6700 and IP8800/S6300] 12
- Troubleshooting System Failures 11

U

- Unable to Input/Display from the Console Correctly 23
- Unable to Obtain Neighboring System Information via LLDP Function 116
- Unable to Obtain Neighboring System Information via OADP Function 116

W

- When Resource Shortage Occurs in Shared Memory 135
- When Resource Shortage of VLAN Identification Table Occurs 133
- Writing to MC 152